Universidad Autónoma de Madrid
Escuela politécnica superior

Grado en Ingeniería de Tecnologías y Servicios de Telecomunicación

Trabajo Fin de Grado

ADQUISICIÓN Y ANÁLISIS DE INFORMACIÓN MANUSCRITA EN ENTORNOS MÓVILES

Autor: Javier Gismero Trujillo
Tutor: Rubén Tolosana Moranchel
Ponente: Julián Fiérrez Aguilar

MAYO 2019

ADQUISICIÓN Y ANÁLISIS DE INFORMACIÓN MANUSCRITA EN ENTORNOS MÓVILES

Autor: Javier Gismero Trujillo
Tutor: Rubén Tolosana Moranchel
Ponente: Julián Fiérrez Aguilar

Biometrics and Data Pattern Analytics - BiDA Lab
Dpto. de Tecnología Electrónica y de las Comunicaciones
Escuela Politécnica Superior
Universidad Autónoma de Madrid
MAYO 2019

Resumen

Resumen

El Trabajo de Fin de Grado realizado se enmarca en el campo del reconocimiento biométrico de escritura manuscrita dinámica a través del uso de dispositivos móviles. Hoy en día los métodos de seguridad utilizados en los dispositivos móviles presentan muchas debilidades. Con el objetivo de hacer estos sistemas más robustos, se propone dibujar las contraseñas en vez de teclearlas. De esta forma se puede analizar la información biométrica de la escritura del usuario y tener dos etapas de autenticación.

Este trabajo surge a partir de los buenos resultados obtenidos con la base de datos e-BioDigit realizado por el grupo BiDA Lab, donde se demostró el potencial de este nuevo método. Sin embargo, su trabajo se ve muy limitado dado que en el estudio solo se utilizaron números, un único dispositivo de captura, 2 sesiones de captura y un entorno supervisado.

En este Trabajo Fin de Grado se ha diseñado y capturado una nueva base de datos denominada MobileTouchDB, compuesta de más de 200 usuarios en 94 dispositivos móviles diferentes. Esta base de datos posee información biométrica de escritura en entornos móviles. Los usuarios tuvieron que dibujar más de 70 caracteres y símbolos distintos a lo largo de 6 sesiones espaciadas temporalmente. Una vez adquirida la base de datos, se ha realizado un preprocesado de la misma con el objetivo de eliminar errores. Además, se han analizado los datos con el algoritmo DTW para entender cómo de efectivo y robusto es el trabajo propuesto en comparación con el estado del arte.

Finalmente, se presentan las conclusiones alcanzadas a lo largo de este trabajo, así como las posibilidades que se ofrecen para nuevos enfoques de trabajo futuro.

Palabras Clave

Biometría, escritura manuscrita, contraseñas, PIN, OTP, dispositivos móviles, DTW, MobileTouchDB.

Abstract

The Final Degree Project is part of the biometric recognition of dynamic handwriting through the use of mobile devices. Today, the secure methods used in mobile devices have many weaknesses. In order to make these systems more robust, it is proposed to draw the passwords instead of typing them. In this way you can analyze the biometric information of the user's handwriting and have two stages of authentication.

This work arises from the good results obtained with the database e-BioDigit made by the group BiDA Lab, where it was demonstrated the potential of this new method. However, their work is very limited because only numbers, a single capture device, 2 capture sessions and a supervised environment were used in the study.

A new database called MobileTouchDB, composed of more than 200 users in 94 different mobile devices, has been designed and captured in this Final Degree Project. This database has biometric writing information in mobile environments. Users had to draw more than 70 characters and different symbols over 6 temporarily spaced sessions. Once the database has been acquired, it has been preprocessed in order to eliminate errors. In addition, the data have been analyzed with the DTW algorithm to understand how efficient and robust is the work proposed in comparison with the state of the art.

Finally, the conclusions reached throughout this work are presented, as well as the possibilities offered for new approaches to future work.

Keywords

Biometrics, passwords, PIN, OTP, handwriting,touch biometrics, mobile, DTW, MobileTouchDB database.

Agradecimientos

En primer lugar quiero agradecer mi trabajo a quien no podría haber sido mejor tutor, Rubén Tolosona. Gracias por haberme concedido la oportunidad de trabajar a tu lado todos estos meses haciendo el Trabajo de Fin de Grado. Ha sido todo un placer haber sido tutorizado por Rubén, quien ha estado pendiente de mi en todo momento, ayudándome con todo lo que necesitaba y apostando por mi desde el comienzo. Sin duda es una excelente persona.

Me gustaría agradecer también a toda mi familia y a mi novia Alejandra, por haberme ayudado y animado con todos los proyectos y asignaturas a lo largo de la carrera, sin su ayuda no hubiera sido capaz de conseguir ni la mitad de lo que he conseguido.

Quiero agradecer por último a todas las personas de mi clase con la que he tenido la oportunidad de trabajar codo con codo, estudiar y sufrir. Ha sido un verdadero placer trabajar en equipo y con gente tan valiosa e inteligente. Más allá de los conocimientos adquiridos en la carrera, me llevo buenos amigos y compañeros para siempre. En especial quiero agradecer a Jose Mará Navarro, Ricardo Domingo, David Abreu, Antonio Campoy, Javier Galán y Sergio Vivas por todo el apoyo que me han dado, por todo lo que he aprendido de ellos y por todos los buenos momentos que hemos compartido en estos últimos años dentro y fuera de las aulas.

Muchas gracias a todos.

Javier Gismero Trujillo

Mayo 2019

Índice general

Índice de Figuras

Índice de Tablas

1

Introducción

1.1. Motivación

Durante los últimos años se ha podido observar un crecimiento exponencial en el uso de los smartphones en todas las facetas de nuestra vida. Quién se imaginaba hace diez años que íbamos a pedir que nos trajeran la comida de nuestro restaurante favorito a casa en menos de una hora o realizar una transferencia bancaria a nuestro amigo en cuestión de segundos. Sin embargo, en la mayor parte de aplicaciones, los sistemas de autenticación de usuarios siguen siendo basados en contraseñas o PINs, con sus correspondientes desventajas, por ejemplo, son fáciles de averiguar al estar generalmente relacionados con información personal. Además, se abre la puerta a nuevas brechas de seguridad a través de ataques del tipo *smudge attack* (la deposición de rastros de grasa en la pantalla táctil puede ser utilizada por los impostores para adivinar patrones de bloqueo o contraseñas) y *shoulder surfing* (técnica de ingeniería social utilizada para obtener información confidencial mirando por encima del hombro de la víctima).

Este Trabajo de Fin de Grado supone un primer paso hacia la mejora de los sistemas de autenticación tradicionales mediante el análisis de la información manuscrita en entornos móviles. Como idea inicial, se planteó hacer uso de la base de datos e-BioDigit. Esta base de datos contiene información del comportamiento biométrico en números, mediante un único dispositivo de captura y a lo largo de 2 sesiones. Este escenario mostraba ciertas limitaciones que motivaron a adquirir una nueva base de datos; una base de datos con muchísimos más usuarios, en la que no solo se analizaran números, si no todos los caracteres posibles. Además, se pretendía que cada usuario utilizase su propio dispositivo móvil para realizar las sesiones, que hubieran más sesiones de captura y que el sistema fuese no supervisado.

Tras definir todos los requisitos que esta nueva base de datos tendría, se desarrolló una aplicación en Android con la que poder hacerla realidad. Hoy, esa base de datos cuenta con más de 210 usuarios y con información biométrica de los mismos de gran potencial. Esta nueva base de datos recibe el nombre de MobileTouchDB.

Debido a un estudio previo sobre la cantidad de teléfonos Android frente a los teléfonos Apple, se ha decidido que el desarrollo móvil para obtener la nueva base de datos se haga en Android para obtener así una cantidad de información mayor, y por lo tanto obtener mejores resultados del algoritmo sobre la base de datos en cuestión.

1.2. Objetivos

Dicho Trabajo de Fin de Grado se ha llevado a cabo con el propósito de cumplir los siguientes objetivos:

1. Desarrollo de una plataforma capaz de capturar una nueva base de datos que simule los posibles escenarios de aplicación y las dificultades del mismo, tales como la variabilidad entre múltiples dispositivos y sesiones de captura distanciadas temporalmente. Este desarrollo no solo servirá para poder cumplimentar los siguientes objetivos, si no que servirá también de punto de partida para próximos desarrollos que requieran de una plataforma similar a la propuesta en este trabajo.

2. Preprocesado y limpieza de la nueva base de datos MobileTouchDB con el objetivo doble de eliminar posibles errores de captura y extraer información de interés para su futura implementación en sistemas reales. Dicho preprocesado requiere de verificar exhaustivamente que los datos introducidos por los usuarios son correctos para conseguir unos mejores resultados en el posterior análisis.

3. Realización de experimentos sobre la base de datos MobileTouchDB para analizar y comparar el rendimiento conseguido en escenarios no controlados frente a los tradicionales escenarios de oficina. Este estudio se realizará teniendo en cuenta múltiples dispositivos distintos (+90 distintos) a lo largo de varias sesiones distanciadas temporalmente.

4. Mejorar la seguridad en los dispositivos móviles con el fin de que los usuarios estén más protegidos frente a robos y suplantaciones de identidad.

1.3. Metodología y plan de trabajo

Para alcanzar los objetivos establecidos en este Trabajo Fin de Grado, se ha seguido la metodología que se muestra en la Fig. 1.1, detallada a continuación.

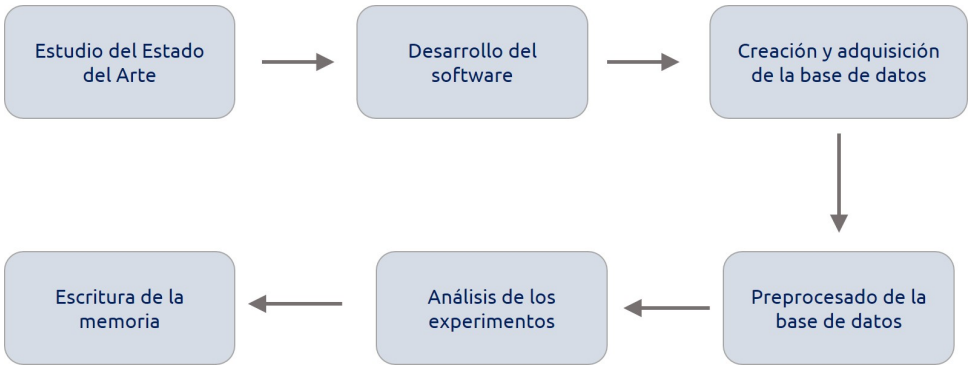


Figura 1.1: Diagrama del plan de trabajo.

- **Estudio del estado del arte:** Para empezar con el trabajo, lo primero de todo ha sido revisar a fondo en qué punto se encuentran los trabajos relacionados y dónde están los límites que a los que se han llegado en este ámbito de estudio. Gracias a este estudio se ha podido, no solo identificar en qué punto nos encontramos, si no aprender nuevos conocimientos y atraer nuevas ideas.

- **Desarrollo del software:** El desarrollo de una aplicación en Android ha sido imprescindible en este trabajo. Este desarrollo ha servido para obtener la base de datos MobileTouchDB. El desarrollo se ha elaborado usando el programa Android Studio, junto a la conexión establecida con ***Firebase***, software de Google que facilita el almacenamiento de bases de datos en la cloud.
- **Creación y adquisición de la base de datos:** Esta nueva base de datos ha sido capturada a través de la aplicación de captura previamente descrita. La base de datos engloba información de todos los números, letras en mayúsculas y minúsculas y diferentes símbolos, abarcando así una cantidad de caracteres distintos muy amplia. Además, dicha captura se ha realizado en un escenario multi-dispositivo, multi-sesión y sin supervisión de nadie. Se ha realizado un análisis previo para lograr que el modo de organizar esta base de datos sea lo más eficente posible.
- **Preprocesado de la base de datos:** Después de tener organizada la base de datos, se ha realizado un preprocesado de la misma, el cual ha resultado de vital importancia ya que se han detectado ciertos errores en algunos usuarios. Estos errores vienen dados pricipalmente porque el dispositivo móvil de ese usuario no esté preparado para reportar toda la información biométrica requerida. Algunos terminales (sobretodo los más longevos) no poseen ciertos sensores como el sensor de presión o giroscopio, y por lo tanto no pueden extraer esa información. La eliminación de este tipo de errores en la base de datos ha sido vital para obtener unos resultados coherentes de los experimentos realizados.
- **Análisis de los experimentos:** Después de todos los pasos anteriores, se ha podido realizar un estudio del comportamiento de los diferentes caracteres a lo largo de las distintas sesiones. Gracias a estos experimentos hemos podido corroborar teorías planteadas previamente y descubrir otras nuevas que no eran de esperar.
- **Escritura de la memoria:** Después de la realización de todos los pasos anteriores, se ha procedido a elaborar la memoria de este Trabajo de Fin de Grado, en la que se pone en comparación el previo estado de arte con los avances realizados a lo largo de este trabajo.

1.4. Organización de la memoria

Este Trabajo Fin de Grado consta de las siguientes secciones:

- **Sección 1:** Introducción
- **Sección 2:** Estado del Arte
- **Sección 3:** Diseño de la Aplicación de Captura
- **Sección 4:** Adquisición de MobileTouchDB
- **Sección 5:** Experimentos Realizados
- **Sección 6:** Conclusiones y Trabajo Futuro

2

Estado del Arte

2.1. Autenticación en la actualidad: Contraseñas

Las contraseñas siguen siendo la forma más común de autenticar usuarios hoy en día. Pueden variar desde Personal Identification Number (PIN) que requieren que los usuarios los memoricen hasta contraseñas de un solo uso (OTP) donde el sistema de seguridad está a cargo de seleccionar y proporcionar al usuario un servicio diferente. Utilizamos las contraseñas diariamente para todo tipo de aplicaciones desde compras on-line hasta transferencias bancarias. Sin embargo, ¿son las contraseñas lo suficientemente seguras? Aparentemente no, al menos por sí mismas. Noticias recientes ponen en evidencia este hecho, por ejemplo, en enero de 2019 un total de 21 millones de contraseñas de todo el mundo fueron expuestas junto con sus correspondientes direcciones de correo electrónico. Este problema no solo afecta a los datos, sino también a otros muchos problemas de seguridad. En el momento en el que un tercero tiene la información necesaria para acceder a un dispositivo móvil o al correo electrónico, puede hacerse pasar por esta persona suplantando su identidad.

En primer lugar, es común utilizar contraseñas basadas en dígitos secuenciales (por ejemplo, "1 2 3 4 5 6"), información personal como fechas de nacimiento, o simplemente palabras como çontraseña.º "qwerty"que son muy fáciles de adivinar. En segundo lugar, las contraseñas que se escriben en dispositivos móviles como tabletas o teléfonos inteligentes son susceptibles de sufrir .ªtaques de borrones", es decir, la deposición de rastros de grasa en la pantalla táctil puede ser utilizada por los impostores para adivinar patrones de bloqueo o contraseñas. Por último, la autenticación basada en contraseña también es vulnerable a la "shoulder surfing". Este tipo de ataque es producido cuando el impostor puede observar directamente o utilizar dispositivos de registro externos para recoger la información del usuario.

Este ataque ha atraído la atención de muchos investigadores en los últimos años debido al creciente despliegue de dispositivos de grabación portátiles e infraestructuras de vigilancia pública. Entonces, si sabemos que las contraseñas tradicionales no son lo suficientemente seguras por sí mismas, pero siguen estando presentes en nuestras vidas, ¿cómo podemos mejorar este tipo de autenticación? Gracias a los avances tecnológicos en el ámbito de la biometría, se pueden aplicar algoritmos sobre las contraseñas tradicionales. De esta manera se consigue mantener el sistema actual incrementando la seguridad de los usuarios.

2.2. Características de los sistemas biométricos

Los sistemas biométricos son los encargados de identificar y analizar patrones y rasgos característicos para poder reconocer la presencia de personas en situaciones muy dispares. Estas situaciones van desde un escenario de personas en movimiento por la calle, hasta escenarios de interacción de las personas con dispositivos móviles. Todo sistema de análisis biométrico se realiza con elementos de captura, como puede ser una cámara o un terminal, y un software capaz de adquirir toda la información de estas características. Algunas de las características de los sistemas biométricos más importantes son las siguientes:

1. **Rendimiento.** Esta característica hace referencia a la precisión, velocidad y robustez con la que es capaz el sistema de dar los resultados. Tiende a ser una característica muy valiosa ya que en términos de seguridad, la robustez frente a amenazas de un programa es uno de los factores clave.

2. **Aceptabilidad.** Este factor indica en qué grado las personas están dispuestas a asumir dicho sistema biométrico en su día a día. La tecnología es una gran herramienta para millones de personas, pero sigue habiendo un gran porcentaje, por lo general de gente más mayor, que tiende a ser reacia a confiar en la tecnología sus bienes más preciados, como puede ser el acceso a su dinero del banco. Por ello, es importante no solo centrarse en el rendimiento del sistema, si no tener en cuenta también este grado de aceptabilidad a la hora de abordar un sistema biométrico.

3. **Fiabilidad.** Por último, esta característica refleja la seguridad con la que el sistema biométrico es dotado. De nada sirve hacer un sistema que sea capaz de trabajar de forma muy precisa y veloz si luego resulta no ser suficientemente seguro. Hoy en día hay técnicas muy avanzas de suplantación de identidad como máscaras, guantes de látex o incluso reconstrucción de huellas que han servido para acceder a sistemas biométricos implantados en dispositivos móviles. Es por ello que el sistema biométrico ha de ser en gran medida muy robusto frente a este tipo de amenazas, ya que asegurando la fiabilidad del sistema, se mejora de la mano su aceptabilidad.

2.3. Trabajos relacionados

2.3.1. Biometría en escritura manuscrita

La biometría mediante el uso de dispositivos móviles se está convirtiendo en una forma muy usual de verificar a los usuarios en sus terminales. A continuación se citan varios estudios relacionados con el tema de la biometría en escritura manuscrita. Para cada estudio, se incluye información relacionada con el método de verificación, características, clasificadores y datasets considerados. También se muestra en la tabla el desempeño de verificación para los dos escenarios de impostores comúnmente considerados en esta área: i) ataque aleatorio, el caso en el que no se conoce información sobre el usuario atacado; y ii) ataque de imitación, el caso en el que los impostores tienen algún nivel de información sobre el usuario atacado. Se debe considerar que la mayoría de los algoritmos y condiciones experimentales varían entre los trabajos listados, por ejemplo, la cantidad y el tipo de datos de entrenamiento y pruebas. Por ello, la tabla debe interpretarse en términos generales para comparar diferentes escenarios de uso basados en la biometría táctil, pero no en pruebas individuales.

En [1] se evalúa el uso de sistemas dinámicos de patrones de bloqueo para la autenticación de usuarios. Para este caso se pidió a los usuarios que dibujaran 3 patrones de bloqueo distintos

Cuadro 2.1: Comparación de los distintos enfoques biométricos de tacto para escenarios móviles.

Estudio	Método	Características	Clasificadores	Rendimiento de Verificación Ataque Aleatorio	Rendimiento de Verificación Ataque de Imitación	# Participantes (Conjunto de Datos)
Angulo *et al.* (2011) [1]	Dinámica del Patrón de Bloqueo	Características Temporales	Random Forest	-	EER = 10.39 %	32
Lacharme *et al.* (2016) [12]	Dinámica del Patrón de Bloqueo	Características Dinámicas	Distancia Hamming	-	EER = 15.0 %	34
Zezschwitz *et al.* (2016) [20]	Dinámica del Patrón de Bloqueo	Características de Forma	Greedy Clustering	-	-	506
Buschek *et al.* (2015) [3]	Pulsación de Teclas	Funciones de Adaptación de Fuentes	Manual	Acc = 94.8 %	-	91
Buschek *et al.* (2015) [2]	Pulsación de Teclas	Características Específicas del Tacto	GM, *k*NN, LSAD	EER = 13.74 %	-	28
Li *et al.* (2013) [8]	Gestos en la Pantalla	Características Estáticas	SVM	EER = 3.0 %	-	75
Sae-Bae *et al.* (2014) [13]	Gestos en la Pantalla	Distancia Entre Puntos	DTW	EER = 1.58 %	-	34
Shen *et al.* (2016) [16]	Gestos en la Pantalla	Características Estáticas	SVM, Random Forest, *k*NN, Neural Networks	EER $\sim$ 3.0 %	-	71
Fierrez *et al.* (2018) [4]	Gestos en la Pantalla	Características Estáticas	SVM, GMM	EER = 10.7 %	-	190
Sae-Bae *et al.* (2014) [14]	Firmas Manuscritas	Características Estáticas	Distancia Manhattan	EER = 5.04 %	-	180
Tolosana *et al.* (2017) [17]	Firmas Manuscritas	Características Dinámicas	DTW	EER = 0.5 %	EER = 17.9 %	65
Khan *et al.* (2011) [6]	Contraseñas Gráficas	Predefined Symbols	Coincidencia Exacta	-	-	100
Martinez-Diaz *et al.* (2016) [10]	Contraseñas Gráficas	Características Dinámicas	DTW, GMM	EER = 3.4 %	EER = 22.1 %	100
Kutzner *et al.* (2015) [7]	Handwritten Password	Características Estáticas y Dinámicas	Bayes-Nets, *K*Star, *k*NN	-	FAR = 10.42 % FRR = unknown	32
Nguyen *et al.* (2017) [11]	Dígitos Manuscritos	Características Dinámicas	DTW	-	EER = 4.84 %	20
Tolosana *et al.* (2018) [19]	Dígitos Manuscritos	Dynamic Features	DTW	-	EER = 5.5 %	93

50 veces (por patrón). Los autores consideraron 11 características relacionadas con el tiempo extraídas del tiempo del dedo en punto y el tiempo entre puntos, logrando resultados por encima del 10.0 % de EER para los ataques de imitación. En [12] se añadieron características biométricas dinámicas relacionadas con la posición del dedo, la presión, el tamaño del mismo y el sensor del acelerómetro a los patrones de desbloqueo tradicionales, logrando obtener un EER final del 15.0 % para los ataques de imitación utilizando un algoritmo de correspondencia basado en la Distancia de Hamming. En [20] se presentó una métrica de similitud para los patrones de desbloqueo en dispositivos móviles para cuantificar el área de contraseñas efectivo de los gestos definidos por el usuario. La métrica propuesta fue evaluada usando más de 500 patrones definidos por el usuario que revelan formas muy similares.

Otros estudios se han centrado en el potencial de la biometría del teclado para la autenticación de usuarios en escenarios móviles. [3] introdujo aspectos cualitativos como el uso de la expresividad personal para mejorar los sistemas biométricos tradicionales de pulsación de teclas. Este sistema se basó en factores cuantitativos como la tasa de error y la velocidad. Incluyeron un marco de personalización dinámica de fuentes, llamado *TapScript*, que adaptaba una fuente dibujada con el dedo según el comportamiento del usuario. Véase entendido el comportamiento como la colocación de los dedos, la orientación del dispositivo y la posición del usuario al escribir. Continuando este enfoque, los usuarios pudieron distinguir pares de mecanógrafos con una precisión del 84.5 % y escenarios de movimiento con un 94.8 %. Estos mismos autores realizaron una comparativa en [2] de las características específicas del tacto entre varias posturas distintas y planes de evaluación: Gaussian Model without covariance (GM), k-Nearest-Neighbours (kNN) y Least Squares Anomaly Detection (LSAD). Los autores llegaron a la conclusión de que las características táctiles espaciales reducen las tasas de error iguales (EER) en un 26.4-36.8 % en comparación con los rasgos temporales tradicionales.

Los sistemas de verificación biométrica basados en gestos de pantalla táctil (es decir, desplazamiento, zoom y clic) en dispositivos móviles están obteniendo alto impacto a día de hoy. Se han propuesto diferentes características y algoritmos en este campo logrando muy buenos resultados contra los ataques aleatorios. En [15] los autores propusieron un conjunto de 22 gestos multitáctiles utilizando características de movimientos de las manos y los dedos con un algoritmo robusto para la orientación y la traslación, logrando un resultado final de 1.58 % de EER. En [4],

un conjunto de 100 características estáticas extraídas de los gestos de deslizamiento y sistemas basados en Support Vector Machines (SVM) y Gaussian Mixture Models (GMM) se consideraron obteniendo rendimientos de hasta un 10.7 % de EER. También se han obtenido muy buenos resultados en [8], [16], utilizando algoritmos de verificación tales como SVM, kNN, Random Forest y Neural Networks. En [18], los autores exploraron el uso de nuevos algoritmos basados en RNNs en escenarios tradicionales para el reconocimiento de firmas, logrando resultados del 5.0 % de EER para ataques de imitación. Sin embargo, se obtiene una degradación considerable del rendimiento del sistema con resultados en torno al 20.0 % de EER para ataques de imitación cuando se prueban en escenarios móviles utilizando el tacto digital como entrada [14],[17]. El motivo principal de esta degradación del rendimiento del sistema es el hecho de que los usuarios tienden a modificar la forma en que firman, por ejemplo, los usuarios que realizan sus firmas utilizando letras cerradas con un lápiz tienden a realizar la escritura mucho más grande cuando utilizan el dedo.

Por último, en [7],[11] los autores propusieron el uso de contraseñas manuscritas para ser autenticadas. En[23], se pidió a los usuarios que realizaran una contraseña de 8 dígitos en la pantalla de un dispositivo móvil. Se extrajeron y probaron 25 características estáticas y dinámicas usando algoritmos de autenticación diferentes. En [11], se evaluó el uso de la biometría escrita a mano para sistemas de autenticación basados en PIN. Su enfoque de autenticación propuesto superó algunos de los inconvenientes anteriormente citados, ya que se pidió a los usuarios que dibujaran los dígitos uno a uno. Se logró un EER final en torno al 5.0 % usando un sistema biométrico compuesto por 5 características dinámicas y un algotithm matcher basado en DTW. Finalmente, un estudio preliminar del trabajo presentado aquí fue publicado en [19]. En ese trabajo realizamos un análisis inicial del sistema biométrico táctil sólo para esquemas de autenticación OTP. Además, DTW fue el único enfoque considerado para el cálculo de la similitud.

2.3.2. Autenticación a través de contraseñas de doble factor

La incorporación de información biométrica en los sistemas tradicionales basados en contraseñas puede mejorar la seguridad a través de un segundo nivel de autenticación de usuarios. Los sistemas de autenticación de dos factores han tenido mucho éxito en los últimos años. Estos enfoques se basan en la combinación de dos etapas de autenticación: i) el sistema de seguridad comprueba que el usuario introduce correctamente su contraseña, y ii) su información biométrica se utiliza para una verificación final mejorada [11], [9]. De esta manera, la robustez del sistema de seguridad aumenta, ya que los impostores no pueden suplantar la identidad únicamente obteniendo la contraseña tradicional. Este enfoque ha sido estudiado en trabajos anteriores. En [1], los autores propusieron un sistema de verificación de dos factores basado en características temporales para patrones, alcanzando un EER final del 10.39 % para los ataques de imitación. En [12] se propuso un enfoque similar de autenticación de dos factores para los sistemas tradicionales de Android. En este caso se tuvo en cuenta características biométricas relacionadas con la posición del dedo, la presión, el dedo y el sensor del acelerómetro alcanzando un EER de 15.0 %. Los enfoques de autenticación de dos factores también se han aplicado a rasgos biométricos fisiológicos. En [5], Jenkins et al. propusieron un sistema basado en las características extraídas para imágenes con rasgos perioculares adquiridas utilizando un dispositivo móvil, logrando así muy buenos resultados en el sistema de identificación.

3

Diseño de la Aplicación de Captura

3.1. Introducción

Se ha creado una aplicación en Android con el objetivo principal de capturar una base de datos con información de biométrica de escritura de cientos de usuarios. El desarrollo en cuestión permite al usuario realizar hasta 6 sesiones en las que el usuario dibuja 72 caracteres distintos y firma dos veces. De este proceso se extrae información como las coordenadas X e Y de la pantalla en cada instante de tiempo, el tiempo que ha tardado en realizar cada carácter, el diámetro de su dedo y otros sensores como el acelerómetro o giroscopio. Después de cada sesión, el usuario envía todo el contenido generado durante la sesión a una base de datos a la que está vinculada la aplicación. Esa base de datos se aloja en *Firebase*, framework de *Google* que facilita la conexión de múltiples usuarios a una base de datos común.

La aplicación fue publicada en *Play Store*, con el objetivo de alcanzar al mayor número de personas posibles y así obtener una base de datos con información de más usuarios. Después de dos meses en *Play Store* y una difusión de la misma en las redes sociales, se alcanzaron alrededor de 300 descargas en diferentes dispositivos, lo que ha permitido obtener unos resultados tras los experimentos bastante fiables. A día de hoy se puede encontrar la aplicación en *Play Store* buscando por e-BioTouch.

3.2. Flujo de la app

El flujo en el que se ha diseñado la aplicación ha sido una de las tareas más importantes en este trabajo. Los usuarios de nuevas aplicaciones tienden a quererlo todo fácil de entender, que no les suponga esfuerzo mental y que la experiencia de usuario sea impoluta. Por ello, se ha llevado un estudio previo en el que se ha analizado cómo interaccionan los usuarios con las aplicaciones móviles, con el objetivo de entender cuáles son los factores que hacen a un usuario descargarse la aplicación y los que hacen que quieran iterar con la misma varias veces. El propósito de la aplicación era que el usuario hiciera las 6 sesiones en la aplicación. Por ello, era crucial que la primera experiencia que tuviera el usuario fuera agradable; de esta manera el usuario haría el resto de sesiones.

El flujo que tras muchos cambios se llevó finalmente a cabo fue el representado a continuacón

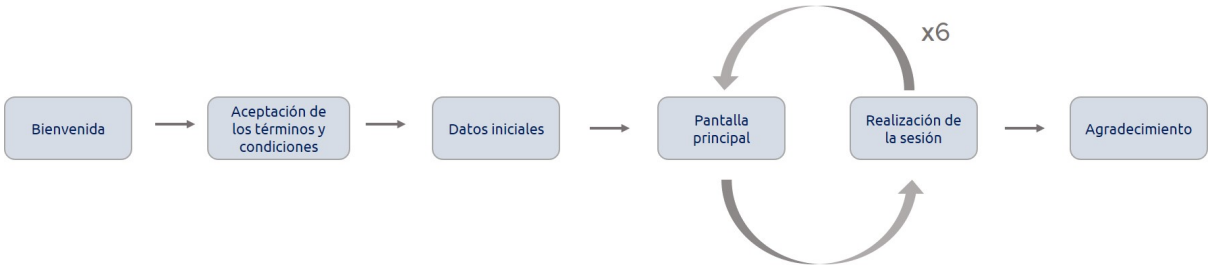


Figura 3.1: Flujo de la aplicación.

en la fig. 3.1. Este flujo nos ha permitido reducir el número de veces que el usuario ha tenido que interactuar con la pantalla para realizar el proceso completo de la aplicación.

- **Bienvenida.** Esta es la etapa inicial, lo primero que ve el usuario al inicial la aplicación por primera vez. En esta interfaz se da la bienvenida al usuario y se describe a modo resumen en qué va a consistir el proceso de las sesiones. Se ha creado una interfaz simple, sin mucha información y con un contenido que deje con ganas al usuario de descubrir los siguientes pasos. En la parte inferior de la pantalla se pide, de forma opcional, el correo de contacto del usuario.

- **Aceptación de los términos y condiciones.** Esta interfaz ha sido utilizada para que el usuario acepte los términos y condiciones de la aplicación en cuestión. En ella, se adjuntaba el link donde encontrar el documento que recoge toda esta información.

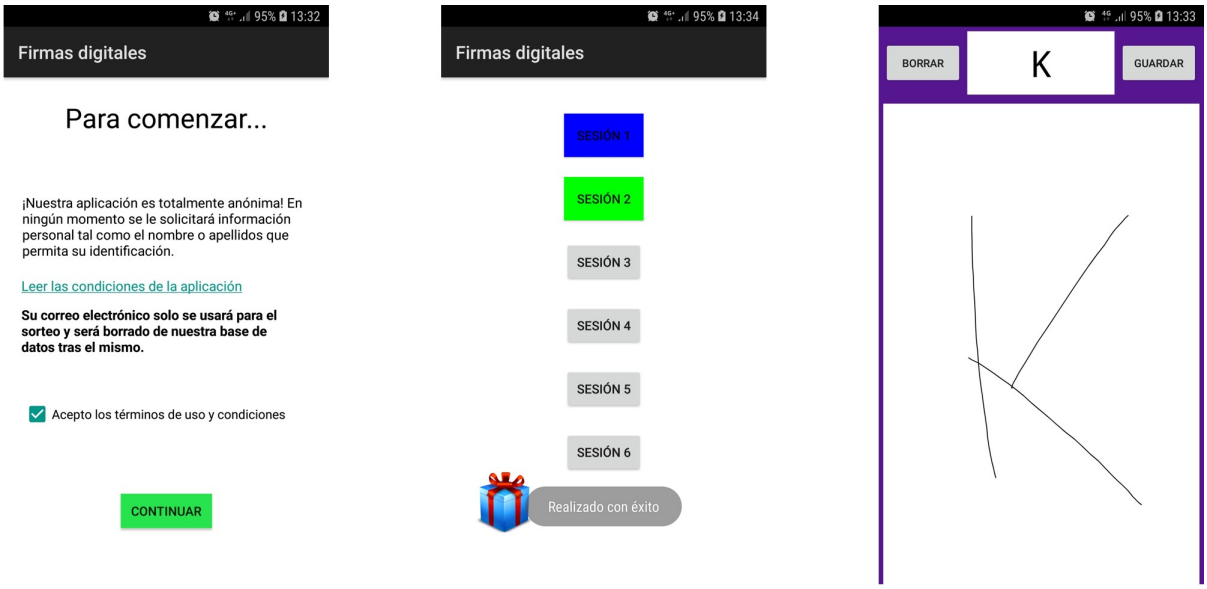
- **Datos iniciales.** En esta etapa, se pedía al usuario que facilitara datos genéricos como su género, edad y mano de escritura. Estos datos han servido, entre otros, para relacionar los resultados de los experimentos con la edad de la gente que he participado.

- **Pantalla principal.** En esta pantalla se puede acceder a las diferentes sesiones a realizar. Cada sesión depende de que la anterior esté hecha. Esto quiere decir que un usuario no podía realizar la tercera sesión, sin previamente haber realizado la primera y la segunda. Adicionalmente, se agregó un botón con el símbolo de interrogación, donde los usuarios podían consultar las preguntas más frecuentes.

- **Realización de la sesión.** Esta es la etapa más relevante. En la parte superior de la pantalla el usuario ve lo que tenía que dibujar. Dándole al botón de borrar podía rehacer su dibujo por si se había confundido, y presionando el botón aceptar avanzaba al siguiente carácter. En total habían 72 caracteres dispuestos de forma aleatoria y compuestos por:

  1. Números del 0 al 9.
  2. Todas las letras mayúsculas del abecedario.
  3. Todas las letras minúsculas del abecedario.
  4. Un total de ocho símbolos como el símbolo de la interrogación y el símbolo de equivalencia.
  5. Composición de cuatro números dispuestos de varias formas.

  El orden en el que aparecían los caracteres era el anterior, pero dentro de cada grupo la distribución era de forma aleatoria. Cuando el usuario terminaba una sesión, regresaba a la pantalla principal de las sesiones. A no ser que la sesión que estuviera realizando fuera la sexta (la última); en ese caso el usuario iría a la última etapa que es la de agradecimiento.



a) Términos de uso y condiciones b) Pantalla principal de las sesiones c) Escritura de los caracteres

Figura 3.2: Capturas de pantalla de la aplicación de captura de la base de datos MobileTouchDB.

- **Agradecimiento.** En esta etapa final se agradecía al usuario el haber realizado todas las sesiones con el tiempo que esto supone, y se le invitaba a rellenar una encuesta de satisfacción para valorar qué le había parecido la experiencia con e-Biotouch.

3.3. Funcionalidades clave

Con el objetivo de caracterizar el desarrollo realizado de la forma más precisa y concisa, se propone resaltar los módulos imprescindibles y más destacados del proyecto. Algunos de ellos han sido adquiridos de Internet y posteriormente modificados y adaptados a nuestro programa; de esta manera se ha conseguido mantener la funcionalidad requerida y al mismo tiempo ajustarla a gusto del programador. Las funcionalidades clave son:

1. **Adquisición de los parámetros biométricos**: Cabe destacar que han habido ciertos dispositivos móviles que han descargado y utilizado e-BioTouch pero no han sido capaces de recoger y guardar toda la información de los parámetros biométricos. Esto se debe a que ciertos terminales especialmente antiguos, cuentan con otras versiones de Android que no les ha permitido extraer el parámetro de la presión, por ejemplo. Sin embargo, concluir que este grupo de terminales no habrá alcanzado el 2 % del total de los mismos en la base de datos MobileTouchDB. Para cada uno de los parámetros extraídos, ha sido necesaria la creación de una o varias funciones específicas capaces en su conjunto de adquirir la información deseada. Los parámetros adquiridos han sido:
   - Posición X e Y de cada muestra adquirida por donde el usuario pasaba el dedo al trazar el carácter.
   - Tiempo entre cada muestra adquirida.
   - Diámetro del dedo sobre la pantalla.
   - Coordenadas del sensor giroscopio para cada muestra.
   - Coordenadas del sensor acelerómetro para cada muestra.

2. **Creación y escritura de ficheros**: Para poder almacenar toda la información detallada en el punto anterior, se ha precisado del uso de ficheros de texto. En estos, la estructura que se ha seguido para ordenar toda la información temporal se dividía por columnas, de tal manera que cada columna alberga la información de un parámetro distinto. El orden de las columnas es exactamente el mismo orden en el que se han enumerado en el apartado anterior, Adquisición de los parámetros biométricos. Cabe destacar que se generaba automáticamente un fichero de texto por cada carácter que el usuario dibujaba.

3. **Almacenamiento en el sistema del usuario**: Una vez explicado cómo se iba a guardar toda la información necesaria, se procede a explicar cómo se organizaba la misma. Lo primero de todo empezaba cuando el usuario abría por primera vez la aplicación. Es en ese momento se generaba una nueva carpeta (en el directorio de aplicaciones de la memoria interna del dispositivo del usuario); en esta carpeta es donde se almacena posteriormente toda la información. Bien, cuando el usuario realizaba una sesión, se generaba en el directorio una nueva carpeta que hacía referencia a la sesión en cuestión. Es en esta carpeta donde, tras cada carácter que el usuario realiza, se genera un nuevo fichero correspondiente a cada carácter. De esta manera se consigue tener de una forma muy ordenada, toda la información que se requiere.

4. **Conexión con la base de datos**: Una vez se termina cada sesión, el usuario envía desde su dispositivo un fichero con toda la información de la sesión en cuestión a una base de datos. De esta manera, se tiene controlada toda la información de todos los usuarios a la vez y en un mismo punto.

5. **Recordatorios**: Con el objetivo de que el usuario no se olvidara de realizar la siguiente sesión después del tiempo establecido entre dichas, se implementó un módulo de recordatorios que funcionaba a través de notificaciones en el dispositivo del usuario. El funcionamiento era el siguiente: el usuario terminaba una sesión y en ese momento se activaba un cronómetro que sabía cuando tenía que darle el aviso al usuario de que ya estaba habilitada la siguiente sesión. Además, si la sesión ya estaba habilitada pero el usuario no la realizaba, se le mandaban recordatorios diarios al usuario para realizar la siguiente sesión. De esta manera, se consiguió que la participación de los usuarios fuese mayor y por lo tanto adquirir una base de datos más robusta.

6. **Temporizador entre sesiones**: Como se ha descrito previamente, el usuario no podía realizar las seis sesiones seguidas, si no que cada sesión se habilitada un tiempo después de realizar la anterior. El motivo principal de esto se debe a que al espaciar temporalmente las sesiones, se adquieren las muestras de los usuarios teniendo en cuenta la variable del tiempo, lo que sitúa un escenario mucho más real de cada a futuras implementaciones. El tiempo entre sesiones era universal para todos los usuarios y era el siguiente:

   - **Sesión 1:** Al descargarse la aplicación.
   - **Sesión 2:** 2 días después de hacer la sesión 1.
   - **Sesión 3:** 2 días después de hacer la sesión 2.
   - **Sesión 4:** 7 días después de hacer la sesión 3.
   - **Sesión 5:** 2 días después de hacer la sesión 4.
   - **Sesión 6:** 2 días después de hacer la sesión 5.

7. **Seguridad ante trampas**: Se quiso prevenir que ciertos usuarios experimentados pudieran avanzar en la aplicación y realizar todas las sesiones seguidas (cosa que alteraría el rendimiento real del sistema). Para ello, la información necesaria para modificar las variables que ajustaban el tiempo que el usuario debía esperar entre sesiones fue ocultado, de

tal forma que no estaba a la vista del usuario y así este no podía modificar a su gusto el tiempo que debía esperar.

3.4. Implementación de Firebase

3.4.1. Introducción

Firebase es la plataforma de desarrollo móvil en la nube de Google. Consiste en una plataforma disponible para diferentes plataformas como *Android*, *iOS* y web. Es fácil de usar, muy potente y con un valor añadido de seguridad que le da la firma *Google*. En este trabajo se ha hecho uso de *Firebase* con dos propósitos principales: i) realizar el envío automático de los ficheros desde el teléfono móvil de los usuarios al servidor de *Firebase*; ii) actuar de base de datos donde almacenar, gestionar y ordenar todos los datos de MobileTouchDB.

Como el escenario de uso de la aplicación no era supervisado, es decir, nadie ha estado controlando ni ayudando a los usuarios, se llevó a cabo la idea de crear un espacio donde toda la información de los usuarios estuviese concentrada en un único punto. De esta manera, se conseguiría recolectar todos los datos de una manera rápida y sencilla, sin tener que molestar al usuario para que transfiera los datos a su ordenador para enviarlos, ni nada por el estilo.

3.4.2. Conexión establecida

Para poder conectar a todos los usuarios que se descarguen e-BioTouch a la plataforma de *Firebase*, es necesario seguir una serie de pasos tanto en el proyecto de *Android* como en la propia web de *Firebase*. Los pasos a seguir son los siguientes:

1. **Crear proyecto en *Firebase*.** Este es el primer paso donde se pone el nombre del proyecto y detalla los términos y condiciones a aceptar para poder usar *Firebase*. Este paso nos dará acceso a los recursos de la plataforma.

2. **Registrar la aplicación.** En este punto se tendrá que elegir el tipo de aplicación con la que conectar. En el caso de este trabajo, la elección es Android. Además, se debe introducir el nombre del paquete de Android, que hace referencia al valor de *ApplicationID* en el archivo *build.grade* del proyecto de Android.

3. **Descargar el archivo de configuración.** Se descargará un archivo llamado google-services.json que se debe incluir en el proyecto de Android. Este archivo permitirá desde el proyecto poder establecer una conexión segura con la sesión de *Firebase* en cuestión.

4. **Añadir el SDK a *Firebase*.** Para que el proyecto de Android ejecute el archivo de configuración descargado previamente, se requiere añadir los comandos que inicializan la conexión con *Firebase*. Esta inicialización se realiza en el fichero *build.gradle*.

5. **Ejecución de la aplicación.** Después de todos los pasos previamente explicados, si se han realizado correctamente ya se podría ejecutar la aplicación y ver desde la plataforma de *Firebase* que la conexión se ha estabilizado correctamente.

3.4.3. Estructura de almacenamiento de los datos

Con el objetivo de almacenar los datos de la forma más sencilla y práctica posible, se ha elegido una forma de estructurar y almacenar los datos que ha sido de gran provecho a la hora de descargar todo el contenido para preprocesarlo y realizar experimentos con ellos.

Dentro de *Firebase*, se ha creado una carpeta llamada *users* donde se alberga toda la información de los usuarios. De esta manera, cuando un usuario termina la primera sesión, se genera una nueva carpeta con su identificador. Dentro de esta carpeta estarán alojados los datos de los caracteres divididos por sesiones. Cuando dicho usuario complete la segunda sesión se guardará la información de la segunda sesión dentro de la carpeta ya existente con el nombre de su usuario.

De esta manera, se puede observar a simple vista cuántos usuarios hay en total y accediendo a cada uno de ellos, cuántas sesiones han realizado y cuándo han hecho cada una de ellas. Se puede concluir que la estructura propuesta ha sido exitosa, ya que el tiempo transcurrido posteriormente para la organización del contenido ha sido mínimo, lo que ha permitido aprovechar ese tiempo para la realización de más experimentos.

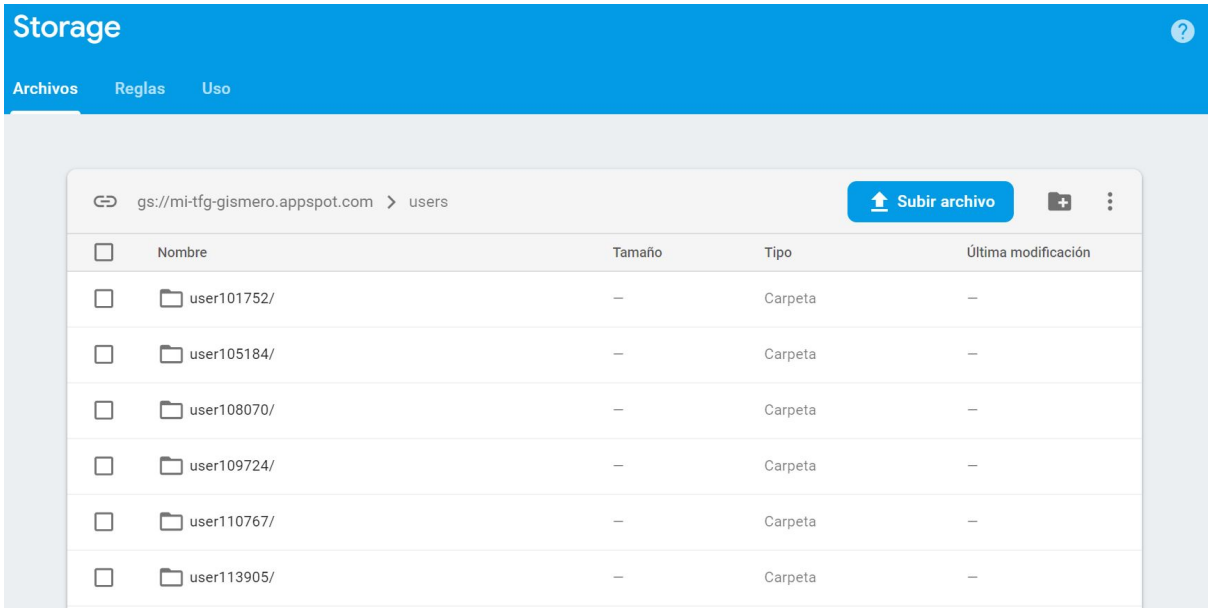


Figura 3.3: Interfaz de la estructura empleada en *Firebase*.

3.5. Encuesta de satisfacción

Una vez el usuario ha completado todas las sesiones de la aplicación, en la interfaz de agradecimiento se le ofrece rellenar un formulario que sirve para recibir feedback del sistema propuesto. Cabe destacar que este formulario lo rellenaron alrededor de 100 usuarios. Se ha usado una herramienta llamada *System Usability Scale (SUS)* (Brooke, 1996) para recopilar evaluaciones subjetivas sobre la usabilidad del sistema propuesto. Cientos de estudios han utilizado el SUS como medida estándar de usabilidad (Bangor et al., 2008, 2009). Además, Tullis et al. encontró que el SUS proporciona los resultados más fiables de la métrica de usabilidad (Tullis y Stetson, 2004). El SUS incluye 10 preguntas en las que la respuesta a cada pregunta se da en una escala de cinco puntos que van desde "muy en desacuerdo" hasta "muy de acuerdo". La nota SUS es un valor comprendido entre 0-100, donde un valor mayor es más deseado porque indica un sistema más utilizable. La puntuación del SUS puede transformarse en un percentil (Sauro, 2011) y una escala de clasificación A-F (Bangor et al., 2008) para mejorar la calidad del resultado. Las 10 preguntas realizadas fueron las siguientes:

1. Creo que me gustaría usar este nuevo sistema de forma frecuente.

2. Pienso que el nuevo sistema sería muy complicado.

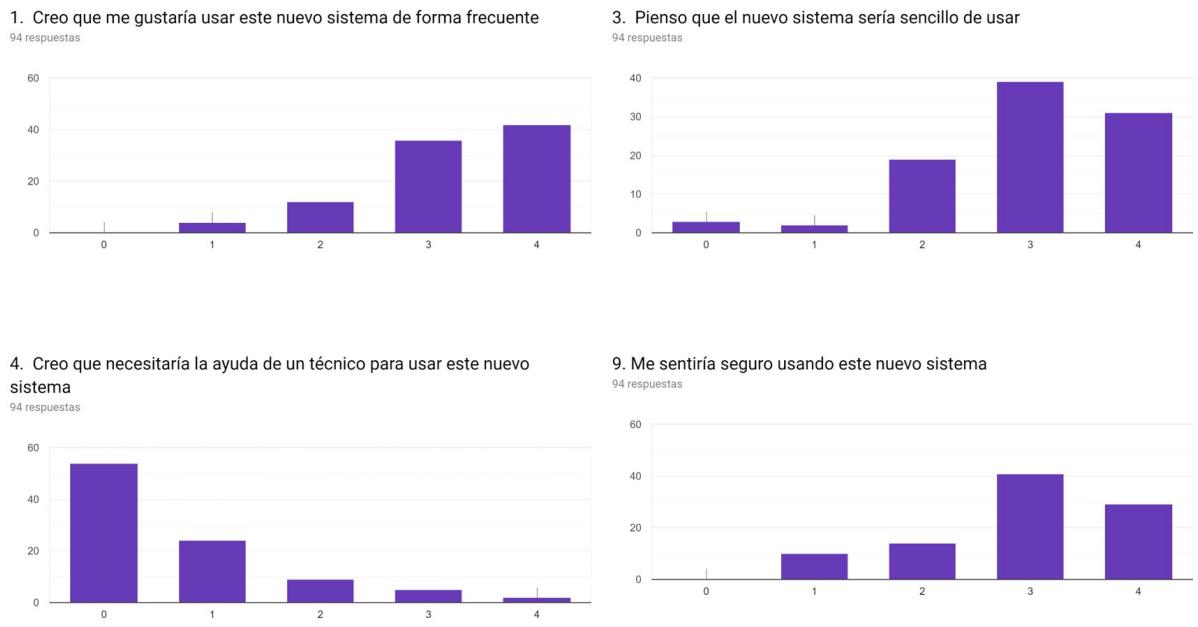


Figura 3.4: Datos encuesta de satisfacción.

3. Pienso que el nuevo sistema sería sencillo de usar.
4. Creo que necesitaría la ayuda de un técnico para usar este nuevo sistema.
5. Creo que la interfaz y el espacio para introducir los caracteres en el nuevo sistema serían los adecuados.
6. Creo que habría mucha inconsistencia en el nuevo sistema.
7. Creo que la mayoría de las personas aprendería a usar este nuevo sistema fácilmente.
8. Creo que encontraría el nuevo sistema muy incómodo de usar.
9. Me sentiría seguro usando este nuevo sistema.
10. Creo que necesitaría muchas instrucciones antes de usar el nuevo sistema.

En general, se alcanza una puntuación del SUS de 74.5, que es mucho más alta que la puntuación media estándar de 68 (Sauro, 2011). Los usuarios también demostraron que probablemente utilizarán el sistema en el futuro. Adicionalmente, se ofrecía de forma opcional, que el usuario añadiera comentarios en un campo de texto al final del formulario, por si se quería añadir algún comentario o idea que no se pudiera plasmar con las preguntas anteriores. Algunos de los resultados que han parecido más interesantes se pueden encontrar en la Fig. 3.3.

4

Adquisición de MobileTouchDB

4.1. Introducción

Hoy en día existen varias bases de datos que recogen información sobre el comportamiento biométrico de las personas al firmar sobre aparatos electrónicos. Estas bases de datos suelen estar limitadas al uso de un único dispositivo para tomar todas las muestras de los diferentes usuarios y en escasas sesiones de captura con el paso del tiempo. Este hecho repercute en unos mejores resultados de los experimentos, ya que no se produce ningún tipo de variabilidad por parte del dispositivo usado, al ser este el mismo para todos. Además, dichas bases de datos se centran en información biométrica exclusivamente de firmas digitales.

Como se ha explicado con anterioridad, el objetivo de realizar un desarrollo en Android ha permitido que los propios usuarios se descarguen la aplicación desde *Play Store*. Esto ha repercutido favorablemente en el estudio ya que se consigue aproximar a un escenario de implementación mucho más realista, donde el usuario no necesita un dispositivo específico para participar en el estudio, si no que lo puede hacer desde su propia casa. Este hecho se ha traducido en un mayor número de muestras frente a las bases de datos actuales. Adicionalmente, es importante recalcar que la información extraída no solo recoge información biométrica de cómo los distintos usuarios realizan su firma, si no de más de setenta caracteres distintos obteniendo así más de dos millones de muestras recogidas en tan solo dos meses de uso por más de doscientos usuarios.

4.2. MobileTouchDB

4.2.1. Características de la base de datos

Para comprender bien las características de la base de datos, se tienen que entender correctamente los siguientes conceptos:

1. Usuario: Cuando se habla de usuario, se hace referencia a aquel que ha descargado la aplicación de Android y ha realizado todas las sesiones de la misma.

2. Sesión: Como se dijo con anterioridad en esta memoria, hay un total de seis sesiones que se realizan consecutivamente con un espacio temporal entre ellas.

Cuadro 4.1: Características más relevantes de las bases de datos públicas biométricas táctiles.

Base de datos	**Método**	**# Usuarios**	**# Sesiones**	**Tiempo de adquisición**	**# Dispositivos**
Serwadda	Swipe	190	2	$\geq$ 1 Día	1
Frank	Swipe	41	2	1 Semana	4
Antal	Swipe	71	-	4 Semanas	8
UMDAA-02	Swipe	48	248	1 Semana	1
DooDB	Contraseñas gráficas	100	2	2 Semanas	1
e-BioDigit	Números manuscritos	93	2	3 Semanas	1
MobileTouchDB	**Caracteres manuscritos**	**217**	**6**	$\geq$ **3 Semanas**	**94**

3. Carácter: En cada sesión, se le pide al usuario que realice diferentes caracteres, un total de 72 caracteres y dos firmas.

A la hora de plantear las características de la base de datos, se realizó un primer estudio sobre la información biométrica que se puede extraer de los dispositivos móviles y qué tan útil es esa información. En la tabla 4.2 se puede observar bases de datos relacionadas con el trabajo en cuestión, que fueron analizadas previamente para entender sus limitaciones y posibilidades. La base de datos diseñada y capturada en este trabajo, MobileTouchDB, consta de las siguientes características:

- **Información personal del usuario.** Esta información se recoge en un fichero de texto y contiene los siguientes parámetros:

  1. Identificador único del usuario.
  2. Edad del usuario.
  3. Sexo del usuario.
  4. Si el usuario es diestro o zurdo.

  Los datos personales del usuario son muy importantes para hacer análisis comparativos entre los parámetros anteriores. Un ejemplo podría ser comparar cómo de robusto es el sistema en función de si la persona que ha realizado las sesiones es zurda o diestra, o en función de la edad de los usuarios.

- **Características biométricas.** Al extraer los datos de una aplicación de Android publicada en *Play Store*, se alcanza información de muchísimos tipos de dispositivos móviles distintos. Esto repercute en que algunos dispositivos pueden no tener ciertos sensores (por lo general, aquellos terminales más longevos) o incluso que éstos no sean capaces de reportar la información de todos los sensores a una frecuencia suficientemente alta como para ser de provecho para realizar experimentos. Contando con este factor, se ha centrado en la extracción de los sensores más genéricos entre todos los terminales y más relevantes a la hora de realizar los experimentos. Dicha información se recoge a continuación:

  1. **Coordenadas X e Y.** Este dato hace referencia a la posición X e Y de los puntos por donde el usuario pasa el dedo para dibujar cada carácter. Con esta información se podrá extraer la primera y segunda derivada de X e Y como *inputs* en el algoritmo utilizado para los experimentos.
  2. **Tiempo.** Este dato hace referencia al tiempo que tarda el usuario en realizar cada carácter individualmente.
  3. **Diámetro del dedo.** En primera instancia se planteó usar el sensor de presión de los terminales como parámetro biométrico a analizar. Sim embargo, este sensor solamente se encontraba disponible en terminales de última generación o de alta gama, por lo que reducía mucho la posibilidad de obtener una base de datos voluminosa con

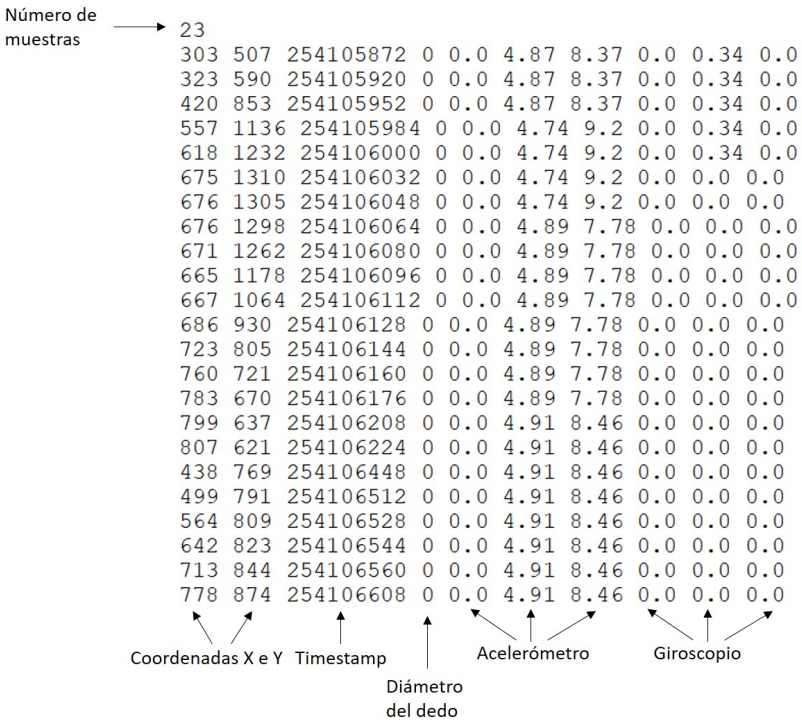


Figura 4.1: Ejemplo de la estructura de almacenamiento en los ficheros.

esta información. Por ello, se eligió como alternativa obtener la información sobre el diámetro del dedo que apoyaba el usuario en la pantalla en cada muestra, ya que puede ser un parámetro altamente discriminatorio.

4. **Sensor Giroscopio.** La información de este sensor viene dada en las coordenadas X, Y, Z. De esta manera se puede comprobar en qué posición de inclinamiento está el terminal en cada momento que está realizando las sesiones.
5. **Sensor Acelerómetro.** La información de este sensor también se extrae en las mismas coordenadas que el sensor giroscopio, sirviendo en este caso para identificar si el usuario está quieto o se va moviendo a lo largo de la sesión o incluso de la realización de los propios caracteres.

Cabe destacar que los parámetros mencionados previamente son datos que se extraen por frecuencia de muestreo en cada carácter; esto quiere decir que son datos que se extraen cada 0.016 segundos aproximadamente (de media, los terminales con menos potencia son capaces de extraer los datos a una frecuencia inferior).

4.2.2. Estructura empleada

La estructura de la base de datos es una tarea muy importante por varios motivos: en primer lugar, para la labor de preprocesamiento de los datos, ya que la base de datos con la que se trabaja es muy voluminosa y es fácil equivocarse a la hora de realizar una modificación o eliminación en la misma si no se tiene clara la estructura de estos datos. Además, a la hora de realizar los experimentos, si los datos están estructurados de una forma determinada se puede conseguir que el rendimiento mejore considerablemente. Uno de los experimentos que se ha llevado acabo tarda en torno a 30 minutos en completarse; si esta labor de estructuración no se hubiera realizado, se podría estar hablando de números mucho mayores, lo que empeora la agilidad con la que se

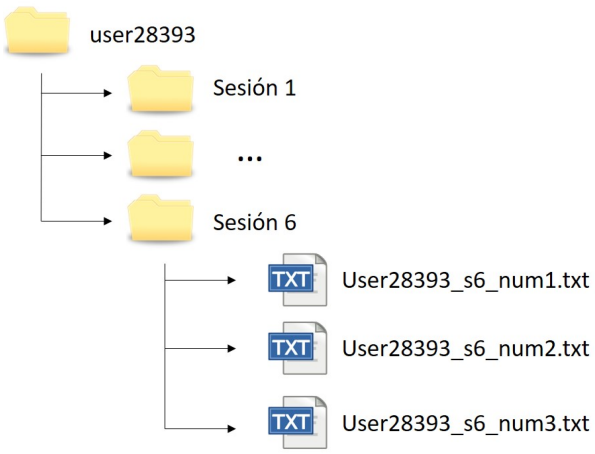


Figura 4.2: Estructura del almacenamiento de los ficheros.

tratan los datos. En la fig. 4.2 se puede apreciar un esquema de la estructura de almacenamiento de los datos.

En cuanto a los datos adquiridos, cada sesión consta de 8 capturas diferentes bloques (es decir, de Bloque 1 a Bloque 8). La Fig. 4.3 muestra algunos ejemplos de cada uno de los ocho bloques de adquisición para dos usuarios diferentes (indicados en colores azul y rojo). Las líneas punteadas verdes indican las trayectorias de las plumas hacia arriba entre los trazos. En el Bloque 1, hace referencia al dibujo de todos los números (del 0 al 9). El Bloque 2 y el Bloque 3 están formados por letras mayúsculas y minúsculas respectivamente, con un total de 27 letras cada uno. El bloque 4 está compuesto por 8 símbolos diferentes (es decir, "?", "#", "*", "@", " %", "=", "ϵ", y "α"). De esta manera, cada usuario realiza una secuencia de caracteres diferente en cada sesión. Desde el Bloque 1 hasta el Bloque 4, la interfaz de adquisición se diseñó en formato vertical para proporcionar una mejor experiencia al usuario. Después de terminar los primeros 4 bloques enfocados en realizar un solo carácter a la vez (una muestra por carácter), se pide a los usuarios que dibujen contraseñas compuestas de 4 números (siempre "5 7 8 4") de diferentes maneras (6 muestras en total).

En el Bloque 5, los usuarios ejecutaron la contraseña dos veces usando una interfaz de orientación horizontal. Se proporciona a los usuarios una visualización gráfica de los números mientras los dibujaban (es decir, en modo visible). Luego, en el Bloque 6, los usuarios tuvieron que repetir una vez la misma tarea considerada en el Bloque 5, pero esta vez en un modo invisible, es decir, no se proporciona a los usuarios cualquier visualización de los números mientras los dibujan. La principal motivación de este nuevo escenario de adquisición es la protección contra los ataques shoulder surfing, como se comentó previamente. En el Bloque 7, los usuarios tenían que dibujar cada número del dentro de cada una de las cuatro casillas disponibles (dos veces), considerando primero un modo visible. Finalmente, en el Bloque 8 los usuarios tenían que repetir una vez la misma tarea considerado en el Bloque 7 pero esta vez en modo invisible. En tanto en el Bloque 7 como en el Bloque 8 se mantuvo la interfaz de adquisición retrato para analizar la experiencia del usuario en diferentes entornos.

4.2.3. Preprocesado de la base de datos

Como se ha explicado con anterioridad, antes de empezar a trabajar en los experimentos es importante realizar un preprocesado de la base de datos. Con el propósito de crear una base de datos de mayor tamaño y características que las actuales, se ha llevado acabo un preprocesado exhaustivo para evitar cualquier error que pudiera surgir. Todos los errores que se han localizado

han sido posteriormente eliminados. Es importante recalcar que como la aplicación en cuestión se ha publicado en *Play Store*, cualquier persona en el mundo con un smartphone Android podía descargarla y usarla de manera no supervisada; por ello, el proceso del preprocesado de la base de datos resulta tan necesario.

Para empezar, se ha analizado en la base de datos que no hubieran usuarios repetidos, ya fuera por un error inesperado en la aplicación o por un intento de réplica por parte de algún usuario. De esta manera, no solo se evitaría contenido repetido que afectara al rendimiento, si no que además se previene de posibles errores a la hora de ejecutar los algoritmos por culpa de elementos repetidos.

En segundo lugar, se han revisado errores en la base de datos referentes a, que por alguna razón, la aplicación no hubiera funcionado correctamente a la hora de recoger la información de las sesiones. Este tipo de error no ha sido muy frecuentado, pero es cierto se ha encontrado en algún usuario una o varias sesiones aparentemente realizadas, pero sin contenido.

Por último y más importante, se ha querido revisar visualmente que los caracteres introducidos por cada usuario eran correctos. Para ello, se ha realizado un script en *Matlab* que recorre la carpeta raíz donde están todos los usuarios, todas sus sesiones y todos sus caracteres. De esta manera, el programa entra en cada sesión de cada usuario e imprime por pantalla a la vez setenta y dos gráficas, haciendo cada una de ellas referencia a cada carácter de cada sesión de cada usuario. El objetivo principal de esta revisión se basa en verificar que cuando la aplicación le ha pedido a un usuario dibujar el número cero, efectivamente haya dibujado ese número y no cualquier otra cosa. Sin duda, este proceso ha sido el más laborioso y mecánico del trabajo en conjunto, ya que se han analizado todos los caracteres de todas las sesiones de todos los usuarios; aproximadamente, se han impreso y revisado unas 50.000 caracteres.

4.2.4. Base de datos en cifras

Los datos que se recogen a continuación hacen referencia a la base de datos después de haber pasado en tratamiento de preprocesamiento comentado en la sección anterior. Dicha base de datos es la que se han aplicado distintos experimentos. En la siguiente tabla se hace una comparativa entre las bases de datos similares en la actualidad, con la obtenida en este trabajo.

Se puede apreciar claramente que la base de datos adquirida resulta bastante competente respecto a las bases de datos relacionadas. Este hecho viene dado, por un lado, por el gran número de usuarios que hemos conseguido atraer para que se descargasen la aplicación de Android y realizaran todas las sesiones. Un total de 217 usuarios completaron la sesión de adquisición S1. S1 y S2 fueron completados por 159 usuarios. Finalmente, un total de 109 usuarios completaron las seis sesiones de adquisición. Esta reducción de participantes entre las sesiones S1 y S6 se produce debido al desafiante escenario de adquisición considerado en este estudio, ya que fue completamente no supervisado y comprendió varias sesiones de adquisición a lo largo del tiempo. En cuanto a la distribución por edades, el 36,2 % de los participantes son menores de 22 años, el 31.9 % tienen entre 22 y 27 años y el 31.9 % restante tienen más de 27 años. En cuanto a la de género, el 63 % de los participantes eran hombres y el 37 % mujeres. El 96 % de los participantes son diestros.

Por otro lado, MobileTouchDB cuenta con una adquisición de información en 94 modelos de dispositivos distintos, entre los que se encuentran las siguientes marcas: Alcatel, Blackberry, BQ, Coolpad, Doogee, Google, Huawei, LeTV, LG, Motorola, OnePlus, Samsung, Sony, UMIDIGI, Xiaomi, y ZTE. Esto repercute en una gran aproximación a un escenario real, ya que hoy en día hay una variabilidad de dispositivos móviles muy alta.

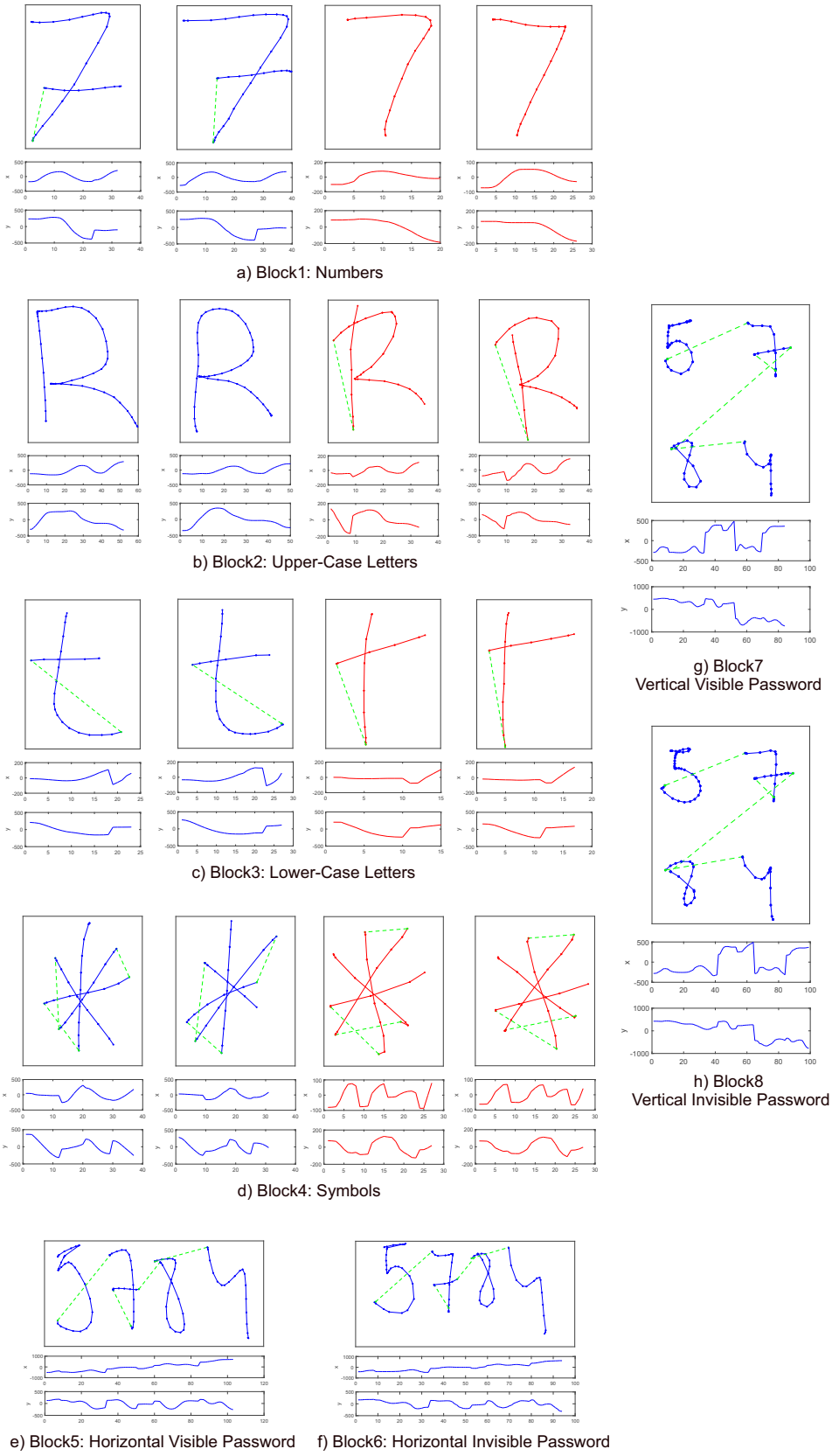


Figura 4.3: Ejemplo de los datos recogidos en la base de datos de MobileTouchDB. Los colores azul y rojo representan las muestras tomadas por diferentes usuarios. Las líneas punteadas verdes indican las trayectorias de las plumas hacia arriba entre los trazos. Las curvas debajo de cada carácter representan X e Y a lo largo del tiempo.

5

Análisis experimental

5.1. Introducción

En los capítulos anteriores se ha descrito el proceso completo que ha permitido adquirir una base de datos de 217 usuarios con características biométricas del comportamiento manuscrito en dispositivos móviles. Gracias a esta voluminosa base de datos, ya no solo por la cantidad de usuarios que han participado, si no por todos los parámetros extraídos, se abre la puerta a infinidad de experimentos. Algunos de ellos se han analizado en este trabajo, pero muchos otros quedan como trabajo futuro y próximos estudios y avances.

5.2. Sistema propuesto

El sistema propuesto se compone de las siguientes etapas:

1. **Extracción de características.** En este trabajo se evalúa el potencial de la biometría en sistemas de verificación basados en funciones temporales. Las señales capturadas por el digitalizador (es decir, las coordenadas espaciales X e Y) se utilizan para extraer un conjunto de 21 funciones de tiempo para cada muestra numérica. No obstante, en este trabajo se hace uso de las funciones temporales relacionadas con las coordenadas X e Y, y sus correspondientes derivadas de primer y segundo orden. La información relacionada con la presión, las orientaciones angulares del lápiz, el ángulo de inclinación del stylus o las alzas del lápiz ampliamente utilizadas en otros rasgos biométricos, como la escritura y la firma manuscrita, no se considera aquí, ya que esta información no está disponible en todos los dispositivos móviles cuando se utiliza la pulsación digital como entrada.

2. **Computación por similitud.** A través del algoritmo Dynamic Time Warping utilizado en este trabajo sigue la descripción proporcionada a continuación.

   La distancia acumulada entre las dos secuencias se calcula de la siguiente manera:

$$D = g(I, J)/K$$

$$g_k = g(i,j) = \min \begin{bmatrix} g(i,j-1) + d(i,j) \\ g(i-1,j-1) + d(i,j) \\ g(i-1,j) + d(i,j) \end{bmatrix}$$

donde K es la longitud de la trayectoria de deformación. Se obtiene una puntuación normalizada como s = exp(-D). Dado un conjunto de muestras de referencia proporcionadas durante la fase de inscripción y una firma de prueba, se calculan las puntuaciones entre todos los datos de referencia y la muestra de prueba y se toma el promedio como la puntuación coincidente para esa muestra de prueba en particular.

5.3. Protocolo experimental

5.3.1. Análisis a nivel de carácter y combinación de caracteres

El protocolo experimental está diseñado para evaluar el potencial de nuestro enfoque biométrico propuesto en escenarios prácticos. Se consideran dos experimentos diferentes: i) análisis de un carácter para evaluar el poder discriminatorio de cada carácter, y ii) análisis de combinación de caracteres para medir la robustez de nuestro enfoque propuesto al aumentar la longitud de las contraseñas de 1 a 9 caracteres. Debido a la gran cantidad de información adquirida en MobileTouchDB, en este trabajo nos centramos en el rendimiento de los caracteres uno por uno. Las contraseñas completas adquiridas en el Bloque 5 al Bloque 8 serán analizadas en estudios futuros.

Las puntuaciones genuinas se obtienen utilizando el conjunto de 159 usuarios con las sesiones de adquisición S1 y S2 completadas. La muestra S1 se utiliza siempre como muestra de entrenamiento, mientras que la muestra S2 se considera como test. De esta manera se considera el problema de la variabilidad entre sesiones, ya que las muestras genuinas de las diferentes sesiones de adquisición se utilizan como muestras de registro y de test respectivamente. Este efecto ha demostrado ser muy importante en muchos rasgos biométricos del comportamiento, como la firma manuscrita, ya que puede simular mejor un escenario real.

Para el escenario impostor, consideramos a los 217 usuarios con la sesión de adquisición de S1 completada. Las puntuaciones de los impostores se obtienen comparando las muestras de entrenamiento de S1 con una muestra de cada uno de los usuarios restantes (de esta manera se simula el escenario en el que el impostor conoce la contraseña).

Finalmente, para el análisis de la combinación de caracteres, la puntuación final se obtiene fusionando las diferentes comparaciones de las puntuaciones de uno a uno utilizando la suma de las puntuaciones.

5.3.2. Análisis del rendimiento con el paso del tiempo

En este experimento se ha tratado de analizar la variabilidad intra-carácter e inter-usuario a lo largo de las sesiones. Como se ha comentario anteriormente en este trabajo, los usuarios han realizado hasta un total de 6 sesiones espaciadas temporalmente. Esto abre la puerta a realizar análisis que tengan que ver con la degradación de estos datos frente al tiempo. Gracias a las 6 sesiones se han podido realizar varias pruebas para comparar el rendimiento de cada una de estas. En este análisis los usuarios que se han utilizado han sido distintos a los utilizados en el experimento anterior, donde se han realizado los siguientes experimentos:

Cuadro 5.1: Conjunto de funciones temporales más usadas en protocolos experimentales.

#	Feature
1	*C*oordenada X: x_n
2	*C*oordenada Y: y_n
3	Trayectoria-ángulo tangente: θ_n
4	Magnitud de la velocidad del trayecto: v_n
5	Radio de curvatura: ρ_n
6	Magnitud total de la aceleración: a_n
7-12	Derivada de primer orden de las características 1-6: $\dot{x_n}, \dot{y_n}, \dot{\theta_n}, \dot{v_n}, \dot{\rho_n}, \dot{a_n}$
13-14	Derivada de segundo orden de las características 1-2: $\ddot{x_n}, \ddot{y_n}$
15	Relación entre la velocidad mínima y la velocidad máxima en una ventana de 5 muestras: v_n^r
16-17	Ángulo de muestras consecutivas y derivada de primer orden: α_n, $\dot{\alpha_n}$
18	Seno: s_n
19	Coseno: c_n
20	Relación longitud/anchura de carrera en una ventana de 5 muestras: r_n^5
21	Relación longitud/anchura de carrera en una ventana de 7 muestras: r_n^7

- Experimento 1. Comparación de las sesiones 1 frente a 6.
- Experimento 2. Comparación de las sesiones 1 y 2 frente a 6.
- Experimento 3. Comparación de las sesiones 1,2 y 3 frente a 6.
- Experimento 4. Comparación de las sesiones 1,2,3 y 4 frente a 6.
- Experimento 5. Comparación de las sesiones 1,2,3,4 y 5 frente a 6.
- Experimento 6. Comparación de las sesiones 2,3,4 y 5 frente a 6.
- Experimento 7. Comparación de las sesiones 3,4,5 frente a 6.
- Experimento 8. Comparación de las sesiones 4,5 frente a 6.
- Experimento 9. Comparación de las sesiones 5 frente a 6.

Para todos los experimentos se utiliza el mismo conjunto de test genuino, S6. De esta manera se empieza comparando S1, como conjunto de entrenamiento, frente a S6. A su vez, para el conjunto de test impostor se consideran a los 217 usuarios con la sesión de adquisición S1 completada. Las puntuaciones de los impostores se obtienen comparando las muestras de entrenamiento de S1 con una muestra de cada uno de los usuarios restantes. Tanto el test genuino como el test impostor son conjuntos de datos que no varían a lo largo de los 9 experimentos.

El motivo de realizar estos experimentos es para comprobar qué tan bueno es el sistema en diferentes escenarios. Se cuestiona con estos experimentos si es más relevante para el sistema usar como conjunto de entrenamiento una sola sesión pero más reciente, o utilizar más sesiones en ese conjunto, más espaciadas en el tiempo.

5.4. Resultados

5.4.1. Análisis a nivel de carácter

La Fig. 5.1 muestra el rendimiento del sistema de cada carácter, agrupado según su bloque de adquisición correspondiente, y de los valores inferiores a los niveles más altos de EER. Primero se analiza en la Fig. 5.1(a) el rendimiento del sistema al dibujar números.

El número "8" alcanza el mejor rendimiento del sistema con un EER del 22.6 %, lo que supone una mejora absoluta del 11.3 % en comparación con el número "6", el cual resulta ser el número menos discriminatorio. Este efecto se produce porque cada persona tiende a realizar caracteres de una manera diferente, es decir, empezando por una zona distinta o incluso la eliminación de algunos de ellos, tales como el trazo horizontal cruzado del número "7".

Los símbolos también son muy discriminatorios. En la Fig. 5.1(b) se muestra la EER alcanzada para cada uno de ellos. En general, los símbolos proporcionan una EER media del 27.2 %, lo que supone una mejora absoluta del 1.8 % en comparación con las cifras, por lo tanto, una mayor capacidad discriminatoria contra impostores. Se cree que esta mejora se debe a que los símbolos como " %" y "*" están compuestos de más trazos, proporcionando una mayor variabilidad entre usuarios. Ahora comparamos los resultados de las letras mayúsculas y minúsculas de la Fig. 5.1(c) y (d). Análisis de la media EER, las letras minúsculas proporcionan una mejora absoluta de 1.0 % EER en comparación con las letras mayúsculas, lo que demuestra que es mayor el poder discriminatorio de las minúsculas. Se cree que esto se produce porque la mayoría de las letras mayúsculas están basado en trazos simples y rectos, y no en trazos curvos, con lo que se consigue una menor variabilidad entre los usuarios. Además, se suele escribir con letras minúsculas, adaptando el modelo de escritura original con características más específicas del usuario en comparación con las letras mayúsculas. Un ejemplo que justifica esta aclaración es la letra "f/F". En la Fig. 5.1(d), la letra "f" indica el mejor resultado con una EER del 19.5 %. Sin embargo, en la Fig. 5.1(c), la EER aumenta hasta el 28.3 % si se utiliza la letra "F". Conclusiones similares se aplican a otras letras como "r/R" y "S/Y". Sin embargo, hay algunos casos en los que tanto las mayúsculas como las minúsculas obtienen resultados muy similares, tales como las letras "x/X" y "g/G" con resultados inferiores al 22.0 % EER.

En general, los buenos resultados de autenticación se obtienen teniendo en cuenta que consideramos un sistema de línea de base basado en en un conjunto simple y fijo de funciones de tiempo para todos los caracteres. En cuanto al poder discriminatorio de cada carácter, se produce una alta variabilidad entre ellos, por ejemplo, hay una mejora absoluta del 17.6 % en la EER entre la letra "f" en la Fig. 5.1(d) y la letra "U" en la Fig. 5.1(c).

5.4.2. Análisis a nivel de la combinación de caracteres

Analizando los resultados obtenidos en la Fig. 5.2, se consigue una mejora considerable del rendimiento del sistema al aumentar la longitud de la contraseña. Una contraseña compuesta de sólo dos caracteres alcanza una EER del 16.4 %, un valor absoluto. una mejora del 3.1 % en el EER en comparación con el caso de la utilización de un con un solo carácter. Este resultado es aún mayor mejorado al aumentar la longitud de la contraseña de de 1 a 9 caracteres, alcanzando una EER final del 5.9 %, un valor absoluto. mejora del EER del 13.6 % en comparación con el caso de la utilización de un solo carácter.

Nuestro enfoque propuesto se compara ahora con el estado del arte del enfoque biométrico de última generación presentado en CVPRw 2018. La información relacionada con el número de muestras de formación consideradas por usuario, la longitud de la contraseña y el rendimiento de verificación en términos de EER se incluye en la tabla para completarla. El estudio presentado

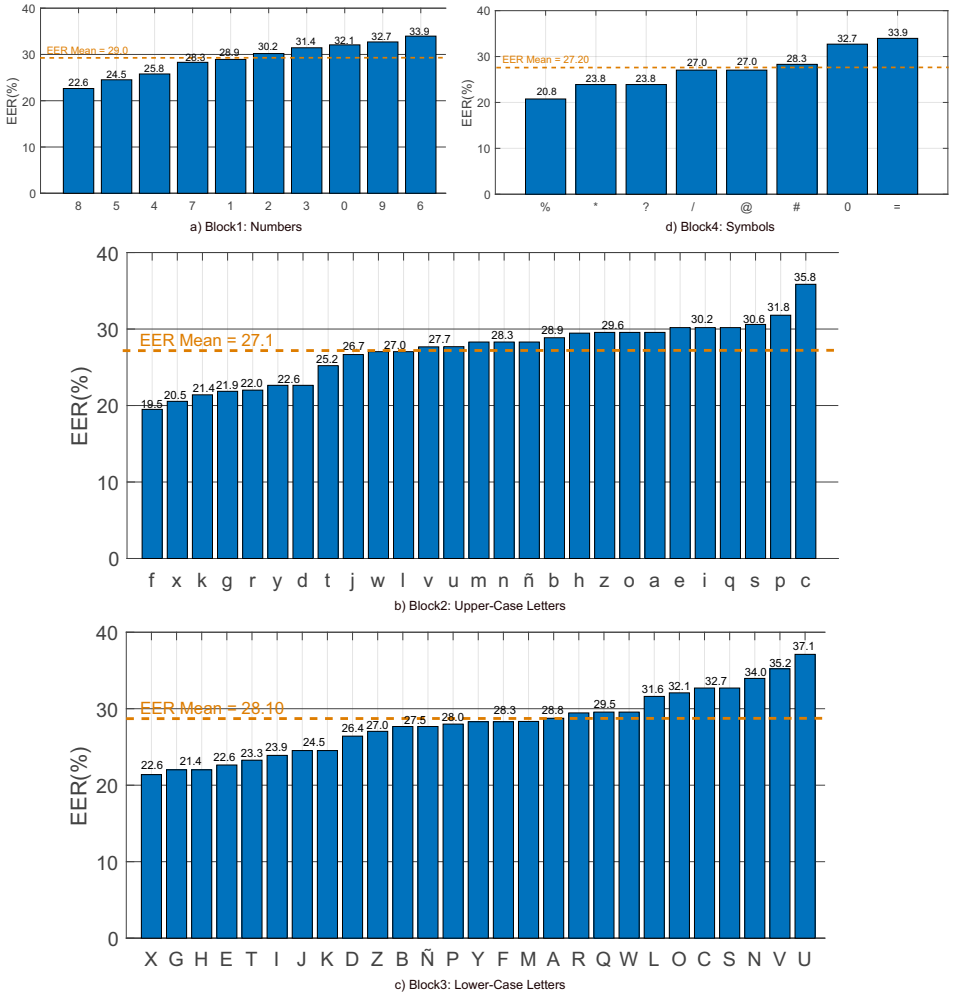


Figura 5.1: Rendimiento del sistema como EER(%) de cada carácter individual. (a) Bloque 1: Números. b)Bloque 4: Símbolos. (c) Bloque 2: Letras mayúsculas. (d) Bloque 3: Letras minúsculas.

aquí ha mejorado aún más el trabajo existente hasta el momento. En este, los autores analizaron el poder discriminatorio de los números adquiridos a través de una tableta de Samsung Galaxy Note 10.1 en un escenario supervisado. El mejor rendimiento del sistema alcanzado fue del 9,0 % EER. En el presente estudio, este resultado se ha mejorado aún más, alcanzando una TEE final del 5,9 % en condiciones experimentales más prácticas (escenario no supervisado con 94 tipos diferentes de smartphones). Este resultado demuestra el mayor poder discriminatorio de los caracteres y símbolos para la tarea de autenticación de usuarios, ya que sólo se consideraron los números, mientras que en el presente estudio no se incluyen números en las mejores combinaciones de contraseñas (es decir, "f x X % k G H g r").

Por último, nos preguntamos cómo el tacto biométrico que se presenta aquí podría proteger a los usuarios en situaciones prácticas. La Tabla 3 muestra el rendimiento del sistema en términos de EER(%) para algunas de las 10 contraseñas más comunes de 2018[15]. Es importante destacar el escenario de impostor considerado, ya que los atacantes conocen la contraseña. En este estudio se obtienen resultados entre 10-17 % EER al incluir una segunda etapa de autenticación basada en la información biométrica táctil de los usuarios. Estos resultados fomentan el despliegue de nuestro enfoque propuesto en comparación con los sistemas tradicionales, donde el ataque tendría una tasa de éxito del 100 % bajo el mismo escenario impostor.

Cuadro 5.2: Comparación de diferentes enfoques táctiles móviles de caracteres escritos a mano en bases de datos públicas.

Trabajo	**Training Samples**	**Longitud de las Contraseñas**	**Rendimiento (EER)**
CVPR 2018 *et al.*	1	9	9.0 %
Enfoque Propuesto	**1**	**9**	**5.9 %**

5.4.3. Análisis del rendimiento con el paso del tiempo

El primer lugar, se puede observar en la Fig. 5.3 cómo ha variado el EER en función del tipo de carácter (números, letras mayúsculas, letras minúsculas y símbolos) y en función de las comparaciones entre sesiones realizadas. Esta gráfica resulta de gran interés porque de ella se pueden extraer don conclusiones muy valiosas:

1. Qué tipo de carácter funciona mejor. Independientemente de las sesiones, se puede apreciar que los símbolos son el tipo de carácter que menor EER consigue, y por tanto mejor rendimiento está presentando. Las letras en minúscula se encuentran un poco mejor posicionadas que las letras mayúsculas; este efecto se produce porque existe una mayor variabilidad entre las minúsculas y las mayúsculas por regla general, de ahí que sea más discriminativa.

2. Rendimiento en función de las comparativas. Se puede observar que los cuatro grupos tienden a reducir su EER en las comparativas más cercanas a la sexta sesión. Una de las conclusiones es que usando la sesión 6 de test y la sesión 5 como entrenamiento va a conseguir mejores resultados que utilizar la sesión 1. Este efecto se produce porque la diferencia temporal entre la sesión 5 y la 6 es de 2 días. Sin embargo, la diferencia total de tiempo repercute en la variabilidad de todos los caracteres. Otra conclusión muy interesante es que entrenar con los datos de la Sesión 5, utilizando las Sesión 6 de test, consigue mejores resultados que usando más sesiones de entrenamiento de este mismo usuario. Este efecto significa que para el sistema utilizado basado en DTW no parece ser necesario guardar en el sistema muestras del usuario procedente de sesiones de captura antiguas. Además, el hecho de que el usuario se vaya re-entrenando a medida que pasa el tiempo, mejora más y más la seguridad del sistema.

Por otro lado, se ha querido comparar la variabilidad entre sesiones consecutivas, esto es:

- Experimento 1. Comparación de las sesiones 1 frente a 2.

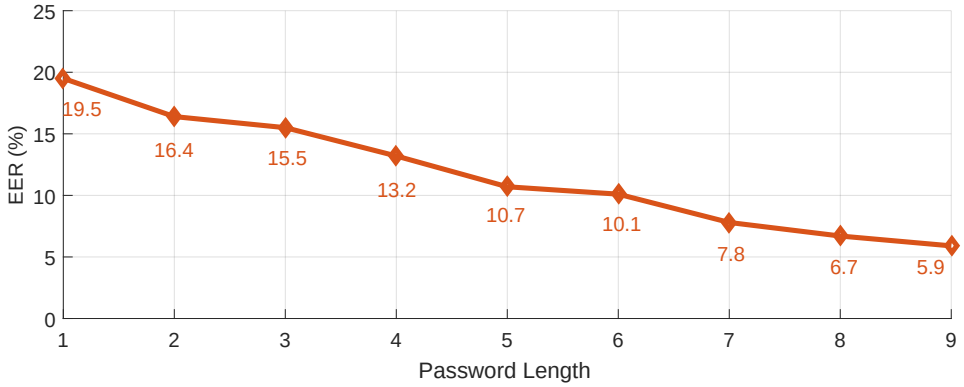


Figura 5.2: Evolución del rendimiento del sistema en términos de EER (%) al aumentar la longitud de la contraseña.

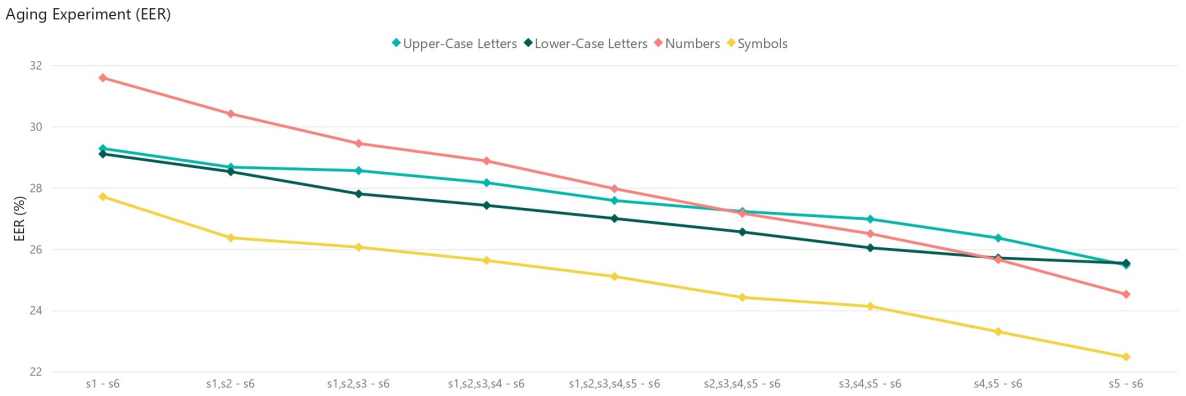


Figura 5.3: Evolución del rendimiento del sistema con diferentes sesiones de train y test.

- Experimento 2. Comparación de las sesiones 2 frente a 3.
- Experimento 3. Comparación de las sesiones 3 frente a 4.
- Experimento 4. Comparación de las sesiones 4 frente a 5.
- Experimento 5. Comparación de las sesiones 5 frente a 6.

Los resultados de esta comparativa se reflejan en la Fig. 5.4, separando el EER por los tipos de caracteres. En estas gráficas se puede extraer una conclusión que hace referencia todos los caracteres: las sesiones consecutivas finales obtienen mejor rendimiento que las primeras. Para la comparativa entre la Sesión 1 y 2 se obtiene de media un EER de 28.02 %, mientras que para la comparativa entre la Sesión 2 y 3 se obtiene un EER de 26.74 % hasta llegar a un EER de 24.52 %. Este hecho lleva a pensar que el usuario a medida que realiza las sesiones, aprende del sistema y en las últimas realiza los caracteres de una forma mucho más similar que al comienzo.

Figura 5.4: Evolución del rendimiento del sistema para sesiones consecutivas.

6

Conclusiones y Trabajo Futuro

En este documento, hemos introducido una nueva base de datos de datos de parámetros biométricos en dispositivos móviles on-line llamados MobileTouchDB. La base de datos contiene más de 64K muestras de caracteres en línea realizado por 217 usuarios, con un promedio de 314 muestras por usuario. En cada sesión de adquisición, los usuarios debían dibujar todos los números (del 0 al 9), letras mayúsculas y minúsculas (54), diferentes símbolos (8) y contraseñas compuestas de 4 números. (6). En cuanto al protocolo de adquisición, MobileTouchDB comprende un máximo de 6 sesiones capturadas por sujeto con un intervalo de tiempo total de al menos 3 semanas. Esta base de datos estudia un escenario móvil no supervisado sin restricciones en términos de posición, postura y dispositivos, ya que los usuarios tenían que descargar y utilizar la aplicación de adquisición en sus propios dispositivos libremente. En este trabajo se ha reportado una evaluación de referencia de la novedosa base de datos MobileTouchDB, que proporciona una fácil framework reproducible. Tres experimentos diferentes se han llevado acabo: i) análisis de un carácter para evaluar el poder discriminatorio de cada carácter; ii) análisis de la combinación de caracteres para medir la robustez de nuestro enfoque propuesto al aumentar la longitud de las contraseñas de 1 a 9 caracteres. Nuestro enfoque propuesto ha sido comparado con la base de datos pública de última generación presentado en CVPRw 2018, alcanzando un EER final del 3.1 %, consiguiendo una mejora absoluta bajo las condiciones de un experimento más práctico (escenario no supervisado con 94 tipos diferentes de los dispositivos móviles), lo que demuestra el mayor poder discriminatorio de caracteres y símbolos para la tarea de autenticación de usuarios; iii) Análisis del rendimiento con el paso del tiempo, donde se ha analizado la variabilidad intra-sesión de los usuarios a lo largo de las semanas que han estado usando la aplicación y realizando así las sesiones. Para el trabajo futuro, se espera reducir aún más el EER a través de técnicas más avanzadas basadas en la selección de características y el aprendizaje profundo. Adicionalmente, se estudiará el poder discriminatorio de las nuevas características adquiridas en la base de datos, así como el área cubierta por el dedo, el acelerómetro o el giroscopio, con el objetivo de mejorar aún más el rendimiento del sistema. Por último, también se analiza la experiencia del usuario en diferentes entornos de adquisición a través del análisis de la información adquirida una vez los usuarios han terminado el proceso completo.

Glosario de acrónimos

- **EER**: *Equal Error Rate*
- **FA**: Falsa Aceptación
- **FR**: Falso Rechazo
- **FAR**: *False Acceptance Rate*
- **FRR**: *False Rejection Rate*
- **DTW**: *Dynamic Time Warping*
- **PIN**: *Personal Identification Number*
- **OTP**: *One Time Password*
- **RNN**: *Recurrent Neutral Networks*
- **SVM**: *Support Vector Machines*
- **GMM**: *Gaussian Mixture Modelling*
- **LSAD**: *Least Squares Anomaly Detection*
- **GM**: *Gaussian Model without covariance*

Bibliografía

[1] J. Angulo and E. Wastlund. Exploring touch-screen biometrics for user identification on smart phones. *Privacy and Identity Management for Life, Springer*, pages 130–143, 2011.

[2] D. Buschek, A. D. Luca, and F. Alt. Improving accuracy, applicability and usability of keystroke biometrics on mobile touchscreen devices. *Proc. of the CHI Conference on Human Factors in Computing Systems*, pages 1392–1403, 2015.

[3] D. Buschek, A. D. Luca, and F. Alt. There is more to typing than speed: Expressive mobile touch keyboards via dynamic font personalisation. *Proc. of the International Conference on HumanComputer Interaction with Mobile Devices and Services*, pages 124–130, 2015.

[4] J. Fierrez, A. Pozo, M. Martinez-Diaz, J. Galbally, and A. Morales. Benchmarking touchscreen biometrics for mobile authentication. *IEEE Trans. on Information Forensics and Security*, 13, 2018.

[5] J. Jenkins, J. Shelton, and K. Roy. One-time password for biometric systems: Disposable feature templates. *Proc. SoutheastCon*, 2017.

[6] W. Khan, M. Aalsalem, and Y. Xiang. A graphical password based system for small mobile devices. *International Journal of Computer Science*, pages 144–155, 2011.

[7] T. Kutzner, F. Ye, I. Bonninger, C. Travieso, M. Dutta, and A. Singh. User verification using safe handwritten passwords on smartphones. *Proc. 8th International Conference on Contemporary Computing*, 2015.

[8] L. Li, X. Zhao, and G. Xue. Unobservable reauthentication for smartphones. *Proc. 20th Network and Distributed System Security Symposium*, 2013.

[9] A. Luca, A. Hang, F. Brudy, C. Lindner, and H. Hussmann. Touch me once and i know its you! implicit authentication based on touch screen patterns. *Proc. of the SIGCHI Conference on Human Factors in Computing Systems*, pages 980–998, 2012.

[10] M. Martinez-Diaz, J. Fierrez, and J. Galbally. Graphical passwordbased user authentication with free-form doodles. *IEEE Trans. on Human-Machine Systems*, pages 600–615, 2016.

[11] T. Nguyen, N. Sae-Bae, and N. Memon. Draw-a-pin: Authentication using finger-drawn pin on touch devices. *Computers and Security*, 66:110–130, 2017.

[12] P. Lacharme C. Rosenberger. Synchronous one time biometrics with pattern based authentication. *Proc. Reliability and Security, ARES*, page 11th, 2016.

[13] N. Sae-Bae and N. Memon. Online signature verification on mobile devices. *IEEE Transactions on Information Forensics and Security*, 9:932–948, 2014.

[14] N. Sae-Bae and N. Memon. Online signature verification on mobile devices. *IEEE Transactions on Information Forensics and Security*, 9:934–948, 2014.

[15] N. Sae-Bae, N. Memon, K. Isbister, and K. Ahmed. Multitouch gesture-based authentication. *IEEE Transactions on Information Forensics and Security*, 9:567–581, 2014.

[16] C. Shen, Y. Zhang, X. Guan, and R. Maxion. Performance analysis of touch-interaction behavior for active smartphone authentication. *IEEE Transactions on Information Forensics and Security*, 11(3), 2013.

[17] R. Tolosana, R. Vera-Rodriguez, J. Fierrez, A. Morales, and J. OrtegaGarcia. Benchmarking desktop and mobile handwriting across cots devices: the e-biosign biometric database. *PLOS ONE*, 2017.

[18] R. Tolosana, R. Vera-Rodriguez, J. Fierrez, and J. Ortega-Garcia. Exploring recurrent neural networks for on-line handwritten signature biometrics. *IEEE Access*, 6:5128–5138, 2018.

[19] R. Tolosana, R. Vera-Rodriguez, J. Fierrez, and J. Ortega-Garcia. Incorporating touch biometrics to mobile one-time passwords: Exploration of digits. *Proc. IEEE Conference on Computer Vision and Pattern Recognition Workshops*, 2018.

[20] E. von Zezschwitz, M. Eiband, D. Buschek, S. Oberhuber, A. D. Luca, F. Alt, , and H. Hussmann. On quantifying the effective password space of grid-based unlock gestures. *Proc. of the International Conference on Mobile and Ubiquitous Multimedia*, pages 200–210, 2016.

A

Artículo aceptado en **IEEE Conf. on Computer Vision and Pattern Recognition Workshops, Long Beach, USA, 2019.**

Previo al desarrollo de la memoria, el trabajo realizado fue presentado como artículo de investigación en el congreso de investigación *CVPR (Computer Vision and Pattern Recognition)*, siendo este aprobado. A continuación, se adjunta el paper en cuestión titulado: *MobileTouchDB: Mobile Touch Character Database in the Wild and Biometric Benchmark.*

MobileTouchDB: Mobile Touch Character Database in the Wild and Biometric Benchmark

Ruben Tolosana, Javier Gismero-Trujillo, Ruben Vera-Rodriguez, Julian Fierrez and Javier Ortega-Garcia
Biometrics and Data Pattern Analytics - BiDA Lab
Universidad Autonoma de Madrid, Madrid, Spain
{ruben.tolosana, ruben.vera, julian.fierrez, javier.ortega}@uam.es, gismerojavi@gmail.com

Abstract

In this paper, we introduce a new database of mobile touch on-line data named MobileTouchDB. The database contains more than 64K on-line character samples performed by 217 users, using 94 different smartphone models, with an average of 314 samples per user. In each acquisition session, users had to draw all numbers (from 0 to 9), upper- and lower-case letters (54), different symbols (8), and passwords composed of 4 numbers (6). Regarding the acquisition protocol, MobileTouchDB comprises a maximum of 6 captured sessions per subject with a time gap between them of at least 2 days. This database studies an unsupervised mobile scenario with no restrictions in terms of position, posture, and devices. Users downloaded and used the acquisition app on their own devices freely. In addition, we also report a benchmark evaluation of biometric authentication on MobileTouchDB, providing an easily reproducible framework for two different scenarios of biometric user authentication: i) based on one character, and ii) based on character combinations.

The database was collected with three main goals in mind: i) analyse the discriminative power of novel human touch interaction dynamics, ii) enhance traditional password authentication systems through the incorporation of touch biometric information as a second level of user authentication, and iii) analyse the way we interact with mobile devices on a daily basis in order to enhance continuous authentication systems. MobileTouchDB is publicly available in GitHub[1].

1. Introduction

Passwords are still the most common way to authenticate users nowadays. They can range from Personal Identification Numbers (PIN) that require users to memorise them to One-Time Passwords (OTP) where the security system is in charge of selecting and providing to the user a different password each time it is required, e.g., sending messages to personal mobile devices or special tokens. We use passwords on a daily basis for all kinds of applications. However, are passwords secure enough? Apparently not, at least by themselves. Recent news put in evidence this fact, e.g., in January 2019 a total of 21 million passwords from all parts of the world were released together with their corresponding emails addresses [12]. This important problem is related not only to data breaches, but also to other many attack scenarios, as it has been pointed out in different studies [6, 10]. First, it is common to use passwords based on sequential digits (e.g., *"1 2 3 4 5 6"*), personal information such as birth dates, or simply words such as *"password"* or *"qwerty"* that are very easy to guess [20]. Second, passwords that are typed on mobile devices such as tablets or smartphones are susceptible to "smudge attacks", i.e., the deposition of finger grease traces on the touchscreen can be used by the impostors to guess lock patterns or passwords [4]. Finally, password-based authentication is also vulnerable to "shoulder surfing". This type of attack is produced when the impostor can observe directly or use external recording devices to collect the user information. This attack has attracted the attention of many researchers in recent years due to the increased deployment of handheld recording devices and public surveillance infrastructures [19, 29]. So, if we know that traditional passwords are not secure enough by themselves, but they continue to be present in our lives, how can we improve this type of authentication?

In this study we introduce the novel MobileTouchDB database and analyse the potential of incorporating touch biometrics to password authentication systems, asking the users to draw each digit of the password on the touchscreen instead of typing them as usual. One example of use that motivates our proposed approach is on internet payments with credit cards. Banks usually send a password (typically between 6 and 8 digits) to the user. This password must be inserted by the user in the security platform in order to com-

[1] https://github.com/BiDAlab/MobileTouchDB

Table 1: Most relevant features of touch biometric public databases.

Database	Method	# Users	# Sessions	Acquisition Time	# Devices
Serwadda [18]	Swipe	190	2	$\geq$ 1 Day	1
Frank [9]	Swipe	41	2	1 Week	4
Antal [3]	Swipe	71	-	4 Weeks	8
UMDAA-02 [14]	Swipe	48	248	1 Week	1
DooDB [15]	Graphical Passwords	100	2	2 Weeks	1
e-BioDigit [21, 24]	Handwritten Numbers	93	2	3 Weeks	1
MobileTouchDB	**Handwritten Characters**	**217**	**6**	$\geq$ **3 Weeks**	**94**

plete the payment. Our proposed approach enhances such scenario by including a second authentication factor based on the user biometric information while drawing the digits.

The main contributions of this study can be summarised as follows:

- We present and describe the acquisition process of the new MobileTouchDB database. The database contains more than 64K on-line character samples performed by 217 users, using 94 different smartphone models, with an average of 314 samples per user. In each acquisition session, users had to draw all numbers (from 0 to 9), upper- and lower-case letters (54), different symbols (8), and passwords composed of 4 numbers (6). Regarding the acquisition protocol, MobileTouchDB comprises a maximum of 6 captured sessions per subject with a total time gap of at least 3 weeks. This database studies an unsupervised mobile scenario with no restrictions in terms of position, posture, and devices. Users downloaded and used the acquisition app on their own devices freely. MobileTouchDB is publicly available in GitHub.

- We report a benchmark evaluation of biometric authentication on the novel MobileTouchDB database, providing an easily reproducible framework. Two different experiments have been carried out: *i)* one-character analysis in order to evaluate the discriminative power of each character, and *ii)* character combination analysis so as to measure the robustness of our proposed approach when increasing the length of the passwords from 1 to 9 characters.

- The MobileTouchDB database opens the doors to many different applications: *i)* analyse the discriminative power of novel human touch interaction dynamics, *ii)* enhance traditional password authentication systems through the incorporation of touch biometric information as a second level of user authentication, and *iii)* analyse the way we interact with mobile devices on a daily basis in order to enhance continuous authentication systems.

MobileTouchDB can be also useful for other research lines beyond touchscreen biometric authentication, e.g.: *i)* user-dependent effects [28], and development of user-dependent methods [7] for handwriting recognition, *ii)* the neuromotor processes involved in writing over touchscreens [13, 27], *iii)* sensing factors in obtaining representative [26] and clean [2] touch interaction signals, *iv)* human-device interaction factors [11] involving touchscreen signals [8], and development of improved interaction methods, and *v)* population statistics around touch interaction signals, and development of new methods aimed at recognising or serving particular population groups [1].

The remainder of the paper is organised as follows. Sec. II summarises public databases in touch biometrics for mobile scenarios. Sec. III describes the design and acquisition process of the MobileTouchDB database. Sec. IV describes the experimental protocol, and the benchmark evaluation carried out. Finally, Sec. V draws the final conclusions and points out some lines for future work.

2. Related Work

The design and acquisition of new databases is always a complex process that requires many efforts for both developers/supervisors and subjects. Not only because of the acquisition process but also due to all the legal aspects that must be carefully tackled to publicly release the data to the research community. Table 1 summarises the most relevant features of different touch biometric public databases.

In [18], the authors acquired a database composed of 190 subjects for the analysis of swipe gestures. Two applications were developed for data collection, running on Android and using one device model (Google Nexus S). In these applications, multiple choice questions were asked based on the images/texts one had to browse/read. Free interaction with the device was allowed, permitting both landscape and portrait orientation. Data were captured over two sessions, at least one day apart, recording the X and Y coordinates, the timestamp, the area covered by the finger, the pressure on the screen, and the device orientation. Only gestures obtained by swiping one finger on the screen were recorded. Multi-touch gestures, e.g. zooms, were ignored.

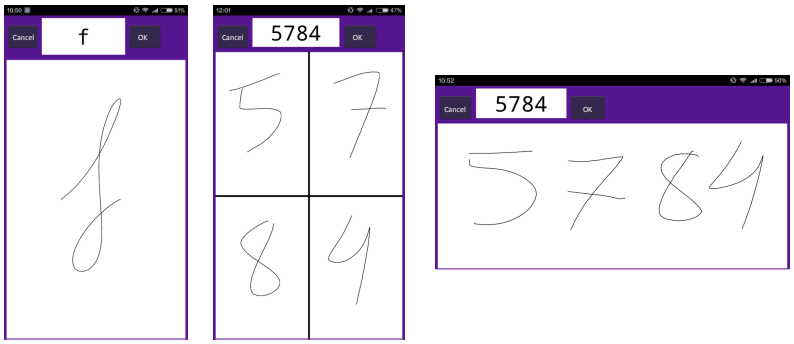


Figure 1: Different interfaces designed for the acquisition app. Both portrait and landscape orientations are considered in order to analyse different user experiences while drawing.

Fran *et al.* acquired in [9] a new database composed of swiping data generated by 41 users over two sessions, one week apart. Two Android applications were deployed for data acquisition, one for comparing images and another for reading texts, allowing the subject to move and interact freely with the screen. Both phone orientations were allowed. Multiple devices (operating on Android) with different sampling frequencies were employed, recording for each data point the X and Y coordinates, the timestamp, the area covered by the finger, the pressure, and the device orientation.

In [3], the authors acquired a new database composed of 71 users. For the acquisition process, eight different devices were used, including tablets with varying screen sizes. An application was developed for the acquisition, where subjects had to read texts, which required vertical swipes, and choose their favourite picture, which required horizontal swipes. The data were obtained during 4 weeks (not separated in sessions in the database), where each subject interacted with multiple devices, recording for each data point the same information as in the previous databases and allowing both phone orientations.

In [14], the authors introduced the UMDAA-02 database, which contains samples from 48 volunteers captured using Nexus 5 phones over two months. On the contrary to the other databases, free use of the devices was allowed during these two months, without requiring any concrete task to be performed. Thus, more data from each user are present. They divided the data in sessions from the unlocking of the device until it was locked again.

Touch biometrics has also been studied in other tasks, e.g., while drawing doodles or numbers [15, 21, 24]. In [15], the authors presented the DooDB, a doodle database containing data from 100 users captured with an HTC Touch HD mobile phone. Doodles were acquired in two different sessions, separated by an average period of two weeks. Finally, more related to the database presented here, we released in [21, 24] the e-BioDigit database composed of 93 users. During the acquisition process, users were asked to draw numerical digits from 0 to 9 on a Samsung Galaxy Note 10.1 tablet in two different sessions with a time gap of at least three weeks between them.

The MobileTouchDB database presented here allows to better analyse the discriminative power of novel human touch interaction dynamics as users had to perform 72 different characters and symbols. Additionally, it considers an unsupervised mobile scenario with no restrictions in terms of position, posture, and devices as users downloaded and used the acquisition app on their own devices freely, simulating this way real scenarios.

3. MobileTouchDB Description

MobileTouchDB is a novel handwritten character mobile touch biometric database composed of more than 64K on-line character samples performed by 217 users. For the acquisition, we implemented an Android application. Fig. 1 represents the different interfaces designed for the acquisition. All interfaces are composed of: *i)* the character/password to draw (top, middle) and two buttons "OK" (top, right) and "Cancel" (top, left) to press after drawing if the sample was good or bad respectively. If the sample was not good, then it was repeated. And *ii)* a rectangular area to perform the character or password. In order to study an unsupervised mobile scenario, the acquisition app was uploaded to the Google Play Store. This way all participants could download and use the app on their own devices without any kind of supervision, simulating a practical scenario in which users can generate handwritten information in any possible scenario, e.g., standing, sitting, walking, indoors, outdoors, etc. As a result, 94 different models from the following 16 brands were used during the acquisition: *Alcatel, Blackberry, BQ, Coolpad, Doogee, Google, Huawei, LeTV, LG, Motorola, OnePlus, Samsung, Sony, UMIDIGI, Xiaomi, and ZTE*. The acquisition app was designed to cap-

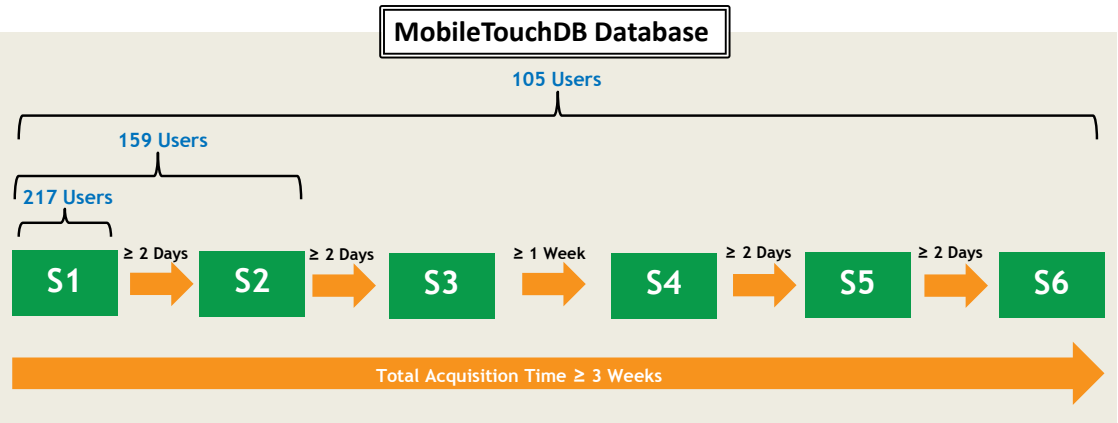


Figure 2: Description of the design and number of available users of the new MobileTouchDB database.

ture the following time signals: X and Y spatial coordinates, the area covered by the finger, timestamp, accelerometer, and gyroscope. However, information related to the area covered by the finger, accelerometer, and gyroscope was not available in some cases depending on how old the acquisition device was.

The acquisition protocol considered in the MobileTouchDB database is depicted in Fig. 2. It comprises a total of 6 sessions (i.e., S1-S6) with different time gaps among them. It is important to highlight that in all sessions, the time gap refers to the minimum time between one user finishes a session and the following session is available. However, participants usually performed their corresponding sessions later on thanks to notifications sent automatically by the acquisition app to the users. Regarding the data acquired, each session comprises 8 different capturing blocks (i.e., from Block1 to Block8). Fig. 3 shows some examples of each of the eight acquisition blocks for two different users (indicated in blue and red colours). The green dashed lines indicate pen up trajectories between strokes. In Block1, we asked users to draw all numbers (from 0 to 9). Block2 and Block3 comprise upper- and lower-case letters respectively, with a total of 27 letters each. Block4 is composed of 8 different symbols (i.e., *"?"*, *"#"*, *"*"*, *"@"*, *"%"*, *"="*, *"ϵ"*, *and "α"*). It is important to remark that inside each block, characters were randomised before asking users to draw them. This way, each user performs a different character sequence in each session. From Block1 to Block4, the acquisition interface was designed as portrait to provide a better user experience (see Fig. 1, left). After finishing the first 4 blocks focused on performing one single character at a time (one sample per character), we asked users to draw passwords composed of 4 numbers (always *"5 7 8 4"*) in different ways (6 samples in total). In Block5, users performed the password twice using a landscape orientation interface (see Fig. 1, right). We provided the users with a graphical visualization of the numbers while drawing them (i.e., visible mode). Then, in Block6, users had to repeat once the same task considered in Block5 but this time in an invisible mode, i.e., we did not provide to the users any visualization of the numbers while drawing them. The main motivation of this novel acquisition scenario is to protect us against shoulder surfing attacks, as commented in [17]. In Block 7, users had to draw each number of the password inside of each of the four available boxes (two times), considering first a visible mode (see Fig. 1, middle). Finally, in Block8 users had to repeat once the same task considered in Block7 but this time in an invisible mode. In both Block7 and Block8 the acquisition interface was kept portrait to analyse the user experience in different settings.

Regarding the MobileTouchDB population statistics, 217 users completed the S1 acquisition session. S1 and S2 were completed by 159 users. Finally, a total of 105 users completed the six acquisition sessions. This participant reduction between S1 and S6 sessions is produced due to the challenging acquisition scenario considered in this study as it was completely unsupervised and comprised several acquisition sessions along time. Regarding the age distribution, 36.2% of the participants are younger than 22 years old, 31.9% are between 22 and 27 years old, and the remaining 31.9% are older than 27 years old. Regarding the gender, 63% of the participants were males, and 37% females. 96% of the population was righthanded.

4. MobileTouchDB Benchmark

This section reports the benchmark evaluation carried out for the MobileTouchDB database, providing an easily reproducible framework. Sec. 4.1 describes all the details of the experimental protocol considered. Then, Sec. 4.2 describes the touch biometric baseline system used in the

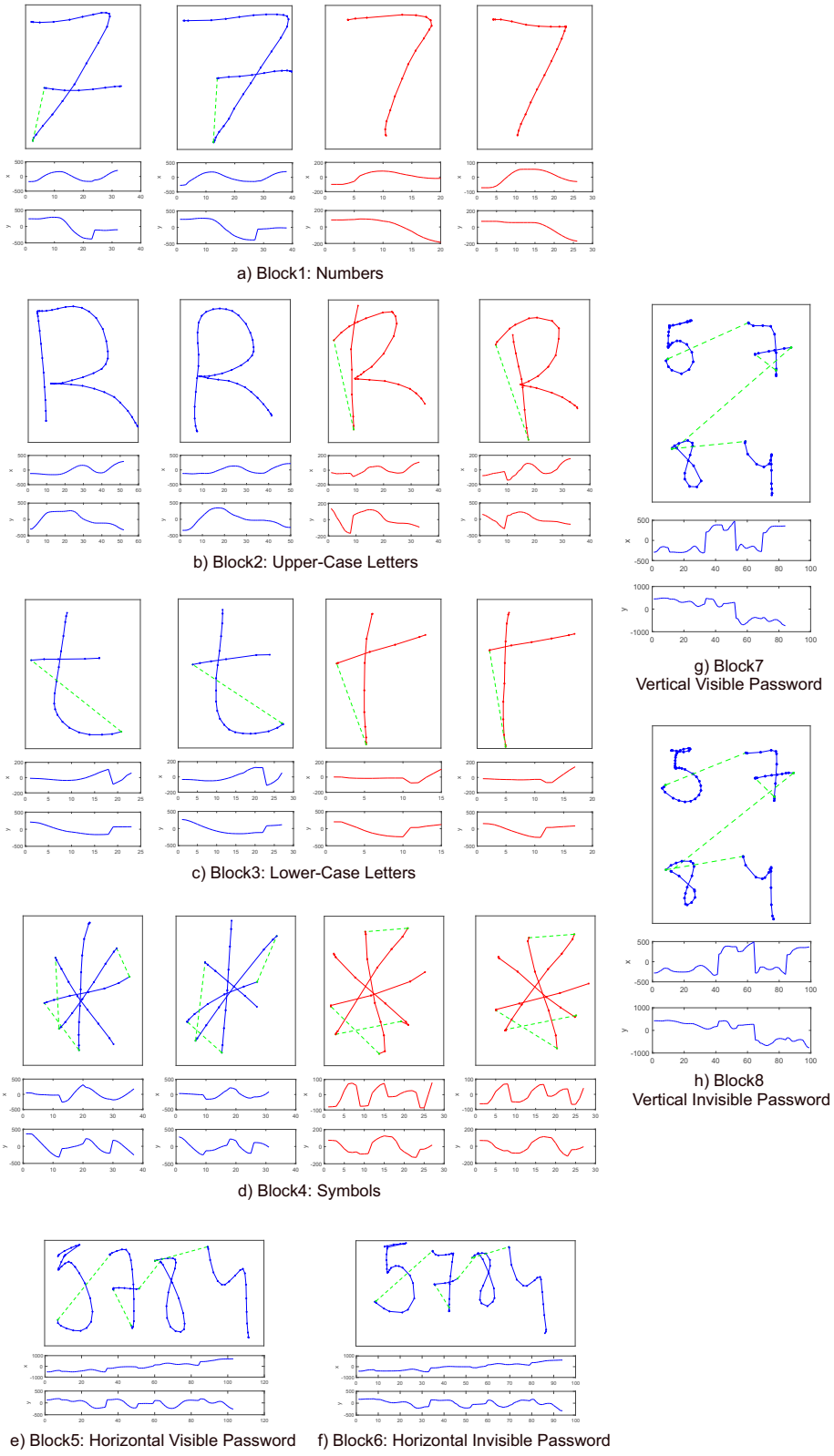


Figure 3: Example of the data collected in MobileTouchDB database. Blue and red colours represent samples drawn by different users. The green dashed lines indicate pen up trajectories between strokes. Curves under each character represent X and Y trajectories over time.

benchmark evaluation. Finally, we analyse in Sec. 4.3 and 4.4 the results obtained for the one-character and character combination scenarios.

4.1. Experimental Protocol

The experimental protocol is designed in order to assess the potential of our proposed password touch biometric approach in practical scenarios. Two different experiments are considered: *i)* one-character analysis in order to evaluate the discriminative power of each character, and *ii)* character combination analysis so as to measure the robustness of our proposed approach when increasing the length of the passwords from 1 to 9 characters. Due to the large amount of information acquired in MobileTouchDB, in this paper we focus on characters performed one at a time. Complete passwords acquired in Block5 to Block8 will be analysed in future studies.

Genuine scores are obtained using the set of 159 users with the S1 and S2 acquisition sessions completed. The S1 sample is always used as training sample whereas the S2 sample is considered for testing. This way we consider the inter-session variability problem as genuine samples from different acquisition sessions are used as enrolment and testing samples respectively. This effect has proven to be very important in many behavioural biometric traits such as the handwritten signature [25], as it can better simulate a real scenario.

For the impostor scenario, we consider all 217 users with the S1 acquisition session completed. Impostor scores are obtained by comparing the training samples from S1 with one sample of each of the remaining users (assuming that the impostor knows the password).

Finally, for the character combination analysis, the final score is produced by fusing the different one by one character score comparisons using the sum of the scores.

4.2. Baseline System

In order to provide an easily reproducible framework, we consider a baseline system based on Dynamic Time Warping (DTW) with the same fixed time functions for all characters. This system is commonly used as baseline in other biometric traits such as the handwritten signature [5, 22]. For each character, we extract the *X* and *Y* coordinates over time and their first- and second-order derivatives, ending up with a set of 6 time functions. For the matcher, DTW is used to compare the similarity between genuine and query input samples, finding the optimal elastic match among time sequences that minimises a given distance measure. Scores are obtained as $score = e^{-D/K}$, where D and K represent respectively the minimal accumulated distance and the length of the warping path [16].

4.3. One-Character Analysis

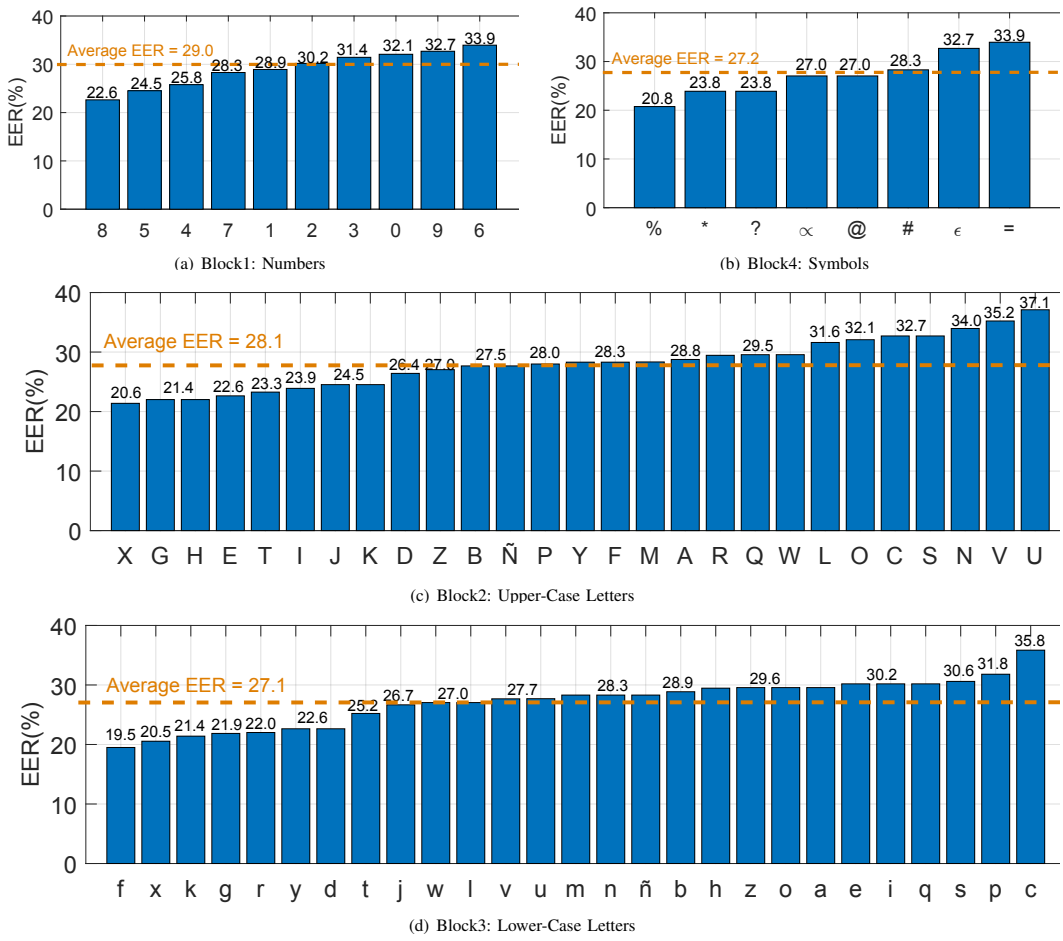
This section analyses the potential of each individual character for the task of user authentication. Fig. 4 shows the system performance of each character, grouped according to their corresponding acquisition block, and from lower to higher EERs.

We first analyse in Fig. 4(a) the system performance when drawing numbers. Number *"8"* achieves the best system performance with a 22.6% EER, an absolute improvement of 11.3% EER compared to number *"6"*, which has resulted to be the least discriminative number. This first experiment puts in evidence the different user verification capacity achieved by each number. Fig. 3 shows examples of the number *"7"* performed by two different users in order to see the low intra- and high inter-user variability of this number. This effect is produced because each person tends to perform characters in a different way, i.e., starting from a different stroke or even removing some of them such as the crossed horizontal stroke of the number *"7"*.

Symbols are shown to be very discriminative as well. Fig. 4(b) depicts the EER achieved for each of them. In general, symbols provide an average 27.2% EER, an absolute improvement of 1.8% EER compared to numbers, achieving therefore a higher discriminative capacity against impostors. We believe this improvement is produced due to symbols such as "%" and "*" are composed of more strokes, providing a higher inter-user variability. Fig. 3 shows examples of the symbol "*" performed by two different users. As it can be seen, users tend to perform symbols in a different way, e.g., starting and finishing in different strokes.

We now compare the results of both upper- and lower-case letters in Fig. 4(c) and (d). Analysing the average EER, lower-case letters provide an absolute improvement of 1.0% EER compared to the upper-case letters, proving the higher discriminative power of lower-case letters. We believe this is produced because most upper-case letters are based on simple straight strokes, and not in curved strokes, providing therefore less variability among users. In addition, we usually write using lower-case letters, adapting our original writing model to more user-specific features compared to upper-case letters. One example that justifies our hypothesis is letter *"f/F"*. In Fig. 4(d), letter *"f"* provides the best result with a 19.5% EER. However, in Fig. 4(c), the EER increases up to 28.3% when using letter *"F"*. Similar conclusions are applied to other letters such as *"r/R"* and *"y/Y"*. However, there are some cases where both upper- and lower-case letters obtain very similar results, such as letters *"x/X"* and *"g/G"* with results below 22.0% EER.

In general, good authentication results are obtained taking into account that we consider a baseline system based on a simple and fixed set of time functions for all characters. Regarding the discriminative power of each character, a high variability is produced among them, e.g., there is an



(a) Block1: Numbers

(b) Block4: Symbols

(c) Block2: Upper-Case Letters

(d) Block3: Lower-Case Letters

Figure 4: System performance as EER(%) of each individual character. (a) Block1: Numbers. (b) Block4: Symbols. (c) Block2: Upper-Case Letters. (d) Block3: Lower-Case Letters.

absolute improvement of 17.6% EER between the *"f"* letter in Fig. 4(d) and the *"U"* letter in Fig. 4(c).

4.4. Character Combinations

This section evaluates the robustness of our touch biometric approach when increasing the length of the password. Fig. 5 shows the evolution of the system performance in terms of EER (%) when increasing the length of the password. Passwords are created following the results extracted in the one-character analysis of Sec. 4.3, including the top ranked most discriminative characters at a time, e.g., the *"f"* and *"x"* letters are used for a two-character password.

Analysing the results obtained in Fig. 5, a considerable system performance improvement is achieved when increasing the length of the password. A password composed of just two characters achieves a 16.4% EER, an absolute improvement of 3.1% EER compared to the case of using a password with just a single character. This result is further improved when increasing the length of the password from 1 to 9 characters, achieving a final 5.9% EER, an absolute improvement of 13.6% EER compared to the case of using a single character.

Table 2: Comparison of different handwritten character mobile touch approaches on public databases.

Work	Training Samples	Password Legth	Performance (EER)
e-BioDigit database [24]	1	9	9.0%
Proposed Approach	**1**	**9**	**5.9%**

Our proposed approach is now compared to the e-BioDigit public database presented in [21, 24]. Information related to the number of training samples considered per user, length of the password, and verification performance in terms of EER is included in Table 2 for completeness. The work presented here has further improved previous studies. In [21, 24], we analysed the discrimina-

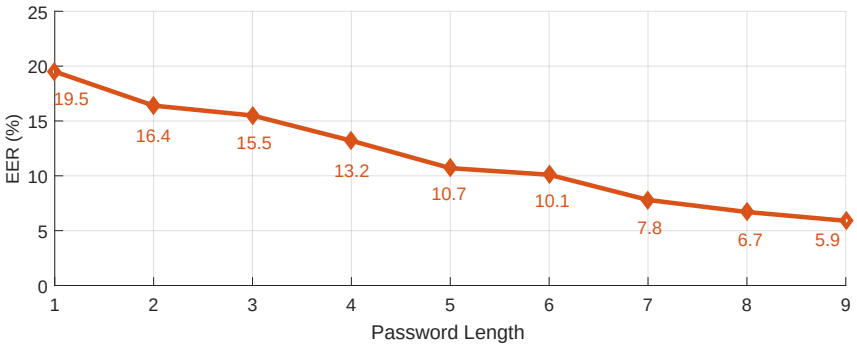


Figure 5: Evolution of the system performance in terms of EER (%) when increasing the length of the password.

Table 3: System performance as EER(%) of five top 10 common passwords of 2018 using our proposed touch biometric approach.

Password	**EER (%)**
123456	17.0
password	13.2
sunshine	12.1
qwerty	12.1
iloveyou	11.3

tive power of numbers acquired through a Samsung Galaxy Note 10.1 tablet in a supervised scenario. The best system performance achieved in [24] was 9.0% EER. In the present study, this result has been further improved, achieving a final 5.9% EER under more practical experimental conditions (unsupervised scenario with 94 different smartphone models). This result proves the higher discriminative power of characters and symbols for the task of user authentication as in [21, 24] only numbers were considered whereas in the present study, no numbers are included in the best password combinations (i.e., *"f x X % k G H g r"*).

Finally, Table 3 shows the system performance in terms of EER(%) for some of the most common passwords of 2018 [20]. It is important to remark the impostor scenario considered as the attackers know the password. Results between 11-17% EER are obtained in this study when including a second authentication stage based on the touch biometric information of the users. These results encourage the deployment of our proposed approach in comparison to traditional systems where the attack would have 100% success rate under the same impostor scenario.

5. Conclusion

In this paper, we have introduced a new database of mobile touch on-line data named MobileTouchDB. The database contains more than 64K on-line character samples performed by 217 users, using 94 different smartphone models, with an average of 314 samples per user. In each acquisition session, users had to draw all numbers (from 0 to 9), upper- and lower-case letters (54), different symbols (8), and passwords composed of 4 numbers (6). Regarding the acquisition protocol, MobileTouchDB comprises a maximum of 6 captured sessions per subject. This database studies an unsupervised mobile scenario with no restrictions in terms of position, posture, and devices. Users had to download and use the acquisition app on their own devices freely. MobileTouchDB is publicly available in GitHub[2].

In this study we have reported a benchmark evaluation of the novel MobileTouchDB database. Two different experiments have been carried out: *i)* one-character analysis, and *ii)* character combination analysis. Our proposed approach has been compared to the e-BioDigit public database presented in [21, 24], achieving a final 3.1% EER absolute improvement under more practical experimental conditions (unsupervised scenario with 94 different smartphone models), proving the higher discriminative power of characters and symbols for the task of user authentication.

For future work, we expect to further reduce the EER through more advanced techniques based on deep learning [23]. Additionally, we will study the discriminative power of new features acquired in the database such as the area covered by the finger, accelerometer, and gyroscope. Finally, we will also analyse the user experience in different acquisition settings through the analysis of the information acquired from Block5 to Block8 of the MobileTouchDB.

Acknowledgments

This work has been supported by projects: BIBECA (MINECO), Bio-Guard (Ayudas Fundación BBVA a Equipos de Investigación Científica 2017) and by UAM-CecaBank. Ruben Tolosana is supported by a FPU Fellowship from Spanish MECD.

[2]https://github.com/BiDAlab/MobileTouchDB

References

[1] A. Acien, A. Morales, J. Fierrez, R. Vera-Rodriguez, and J. Hernandez-Ortega. Active Detection of Age Groups Based on Touch Interaction. *IET Biometrics*, 8:101–108, 2019. 2

[2] F. Alonso-Fernandez, J. Fierrez, and J. Ortega-Garcia. Quality Measures in Biometric Systems. *IEEE Security and Privacy*, 10(9):52–62, 2012. 2

[3] M. Antal, Z. Bokor, and L. Szabó. Information Revealed From Scrolling Interactions on Mobile Devices. *Pattern Recognition Letters*, 56:7–13, 2015. 2, 3

[4] A. Aviv, K. Gibson, E. Mossop, M. Blaze, and J. Smith. Smudge Attacks on Smartphone Touch Screens. In *Proc. of the 4th USENIX Conference on Offensive Technologies*, pages 1–7, 2010. 1

[5] R. Blanco-Gonzalo, R. Sanchez-Reillo, O. Miguel-Hurtado, and J. Liu-Jimenez. Performance Evaluation of Handwritten Signature Recognition in Mobile Environments. *IET Biometrics*, 3:139–146, 2014. 6

[6] J. Bonneau, C. Herley, P. Oorschot, and F. Stajano. The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes. In *Proc. Symp. on Security and Privacy*, pages 553–567, 2012. 1

[7] J. Fierrez, A. Morales, R. Vera-Rodriguez, and D. Camacho. Multiple Classifiers in Biometrics. Part 2: Trends and Challenges. *Information Fusion*, 44:103–112, 2018. 2

[8] J. Fierrez, A. Pozo, M. Martinez-Diaz, J. Galbally, and A. Morales. Benchmarking Touchscreen Biometrics for Mobile Authentication. *IEEE Trans. on Information Forensics and Security*, 13(11):2720–2733, 2018. 2

[9] M. Frank, R. Biedert, E. Ma, I. Martinovic, and D. Song. Touchalytics: On the Applicability of Touchscreen Input as a Behavioral Biometric for Continuous Authentication. *IEEE Transactions on Information Forensics and Security*, 8(1):136–148, 2013. 2, 3

[10] J. Galbally, I. Coisel, and I. Sanchez. A New Multimodal Approach for Password Strength Estimation Part I: Theory and Algorithms. *IEEE Transactions on Information Forensics and Security*, 12:2829–2844, 2017. 1

[11] M. Harbach, A. Luca, and S. Egelman. The Anatomy of Smartphone Unlocking: A Field Study of Android Lock Screens. In *Proc. Conference on Human Factors in Computing Systems*, pages 4806–4817, 2016. 2

[12] T. Hunt. *The 773 Million Record "Collection #1" Data Breach*, 2019. 1

[13] M.A. Ferrer, M. Diaz, C.A. Carmona, and R. Plamondon. iDeLog: Iterative Dual Spatial and Kinematic Extraction of Sigma-Lognormal Parameters. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 2018. 2

[14] U. Mahbub, S. Sarkar, V. Patel, and R. Chellappa. Active User Authentication for Smartphones: A Challenge Data Set and Benchmark Results. In *Proc. Int. Conf. on Biometrics Theory, Applications and Systems*, 2016. 2, 3

[15] M. Martinez-Diaz, J. Fierrez, and J. Galbally. The DooDB Graphical Password Database: Data Analysis and Benchmark Results. *IEEE Access*, 1:596–605, 2013. 2, 3

[16] M. Martinez-Diaz, J. Fierrez, and S. Hangai. Signature Matching. *S.Z. Li and A. Jain (Eds.), Encyclopedia of Biometrics, Springer*, pages 1382–1387, 2015. 6

[17] T. Nguyen, N. Sae-Bae, and N. Memon. DRAW-A-PIN: Authentication Using Finger-Drawn PIN on Touch Devices. *Computers & Security*, 66:115–128, 2017. 4

[18] A. Serwadda, V. Phoha, and Z. Wang. Which Verifiers Work?: A Benchmark Evaluation of Touch-Based Authentication Algorithms. In *Proc. International Conference on Biometrics: Theory, Applications and Systems (BTAS)*, pages 1–8, 2013. 2

[19] D. Shukla, R. Kumar, A. Serwadda, and V. Phoha. Beware, Your Hands Reveal Your Secrets! In *Proc. of the 2014 ACM SIGSAC Conference on Computer and Communications Security*, 2014. 1

[20] SplashData. *The Top 50 Worst Passwords of 2018*. 1, 8

[21] R. Tolosana, R. Vera-Rodriguez, and J. Fierrez. BioTouchPass: Handwritten Passwords for Touchscreen Biometrics. *IEEE Transactions on Mobile Computing*, 2019. 2, 3, 7, 8

[22] R. Tolosana, R. Vera-Rodriguez, J. Fierrez, A. Morales, and J. Ortega-Garcia. Benchmarking Desktop and Mobile Handwriting across COTS Devices: the e-BioSign Biometric Database. *PLOS ONE*, 2017. 6

[23] R. Tolosana, R. Vera-Rodriguez, J. Fierrez, and J. Ortega-Garcia. Exploring Recurrent Neural Networks for On-Line Handwritten Signature Biometrics. *IEEE Access*, 6:5128–5138, 2018. 8

[24] R. Tolosana, R. Vera-Rodriguez, J. Fierrez, and J. Ortega-Garcia. Incorporating Touch Biometrics to Mobile One-Time Passwords: Exploration of Digits. In *Proc. Conference on Computer Vision and Pattern Recognition Workshops*, pages 471–478, 2018. 2, 3, 7, 8

[25] R. Tolosana, R. Vera-Rodriguez, J. Fierrez, and J. Ortega-Garcia. Reducing the Template Aging Effect in On-Line Signature Biometrics. *IET Biometrics*, 2019. 6

[26] R. Tolosana, R. Vera-Rodriguez, J. Ortega-Garcia, and J. Fierrez. Preprocessing and Feature Selection for Improved Sensor Interoperability in Online Biometric Signature Verification. *IEEE Access*, 3:478–489, 2015. 2

[27] R. Vera-Rodriguez, R. Tolosana, and *et al.* Modeling the Complexity of Signature and Touch-Screen Biometrics using the Lognormality Principle. *R. Plamondon, A. Marcelli, and M.A. Ferrer (Eds.), The Lognormality Principle and its Applications, World Scientific*, 2019. 2

[28] N. Yager and T. Dunstone. The Biometric Menagerie. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 32(2):220–230, 2010. 2

[29] Q. Yue, Z. Ling, X. Fu, B. Liu, W. Yu, and W. Zhao. My Google Glass Sees Your Passwords! In *Black Hat USA*, 2014. 1